

Administrative Record Index
USCIS Request for Emergency Paperwork Reduction Act (PRA) Clearance for USCIS
Form I-131F, Application for Parole in Place for Certain Noncitizen Spouses
and Stepchildren of U.S. Citizens
ICR Reference Number 202407-1615-002

Description	Page No.
Memorandum from Samantha Deshommes, USCIS, to Richard Revesz, OIRA, Request for Emergency OMB Paperwork Reduction Act (PRA) Clearance – USCIS Form I-131F, Application for Parole in Place for Certain Noncitizen Spouses and Stepchildren of U.S. Citizens (Aug. 14, 2024)	1
Supporting Statement for Application for Parole in Place for Certain Noncitizen Spouses and Stepchildren of U.S. Citizens (Aug. 14, 2024)	3
Reference Citations (Aug. 14, 2024)	13
Privacy Threshold Analysis (PTA) (Aug. 14, 2024)	14
DHS/USCIS/PIA-056(a), Privacy Impact Assessment for the USCIS Electronic Immigration System (USCIS ELIS) (Dec. 3, 2018)	32
DHS/USCIS/PIA-071, Privacy Impact Assessment for the myUSCIS Account Experience (Dec. 15, 2017)	68
DHS, <i>Privacy Act of 1974; System of Records</i> , 84 Fed. Reg. 54662 (Oct. 10, 2019) (Benefits Information System)	94
DHS, <i>Privacy Act of 1974; System of Records</i> , 83 Fed. Reg. 36950 (July 31, 2018) (Immigration Biometric and Background Check System)	102
DHS, <i>Privacy Act of 1974; System of Records</i> , 82 Fed. Reg. 43556 (Sept. 18, 2017) (Alien File, Index, and National File Tracking System)	108
Notice of Office of Management and Budget Action (Aug. 16, 2024)	118

U.S. Department of Homeland Security
U.S. Citizenship and Immigration Services
Office of Information Technology
Washington, DC 20529



U.S. Citizenship
and Immigration
Services

Memorandum

TO: Richard Revesz
Administrator,
Office of Information and Regulatory Affairs,
Office of Management and Budget

THROUGH: Eric Hysen
DHS Chief Information Officer

FROM: Samantha Deshommes
USCIS Office of Policy and Strategy,
Chief, Regulatory Coordination Division

SUBJECT: Request for Emergency OMB Paperwork Reduction Act (PRA) Clearance – USCIS Form I-131F, Application for Parole in Place for Certain Noncitizen Spouses and Stepchildren of U.S. Citizens.

ERIC N HYSSEN Digitally signed by ERIC N HYSSEN
Date: 2024.08.14 09:45:25 -04'00'

SAMANTHA L DESHOMMES Digitally signed by SAMANTHA L DESHOMMES
Date: 2024.08.13 11:43:37 -04'00'

Purpose: U.S. Citizenship and Immigration Services (USCIS) requests emergency approval for Form I-131F, Application for Parole in Place for Certain Noncitizen Spouses and Stepchildren of U.S. Citizens, a new collection of information. USCIS is seeking approval for the collection of information under 5 C.F.R. § 1320.13(a)(2)(ii) and (iii).

Background: Family unity is a bedrock objective of the U.S. immigration system. While U.S. immigration law generally provides noncitizens who are married to U.S. citizens with the opportunity to apply for lawful permanent resident (LPR) status while remaining in the United States, the requirement to be inspected and admitted or paroled prevents many families from availing themselves of this benefit, even though they otherwise qualify for LPR status.

Recognizing the hardships that American families and communities face as a result of obstacles such as this, President Joseph R. Biden in 2021 directed the U.S. Department of Homeland Security (DHS) and other agencies to “identify barriers that impede access to immigration benefits and fair, efficient adjudications of these benefits and make recommendations on how to remove these barriers as appropriate and consistent with applicable law.”ⁱ

Furthermore, on June 18, 2024, President Biden announced that DHS would take action to preserve the unity of mixed status families by establishing a process for certain noncitizen spouses and stepchildren to

access LPR status without requiring them to depart the United States. DHS is now working to implement that process and open it up for applications by August 19, 2024.

Discussion: Consistent with the President's announcement, DHS is establishing a process for certain noncitizens who are married to a U.S. citizen (or are the noncitizen stepchild of a U.S. citizen) and are present in the United States without admission or parole, to request parole in place under section 212(d)(5)(A) of the INA, 8 U.S.C. § 1182(d)(5)(A).

DHS is publishing a notice in the *Federal Register* titled, "Implementation of Keeping Families Together" and creating Form I-131F, Application for Parole in Place for Certain Noncitizen Spouses and Stepchildren of U.S. Citizens, to implement this process as an online, electronically filed collection of information. Form I-131F will be used by eligible noncitizens to request parole in place under this process.

Establishing the new Form I-131F is essential to the effective adjudication of parole in place requests and subsequent immigration benefit requests submitted by eligible individuals. Emergency processing is justified because USCIS must quickly collect the requested information to fulfill its mission of implementing the President's announcement and meet public expectations that USCIS will begin accepting applications by August 19, 2024. In addition, for various reasons, significant public harm is reasonably likely to result if USCIS were to seek public comment before the process is implemented. First, the hardships these families have endured will continue, undermining the President's directive to eliminate barriers to the immigration system and promote family unity and security. Second, individuals who may be considered for parole in place under this process are already susceptible to fraud perpetrated by consultants and others seeking to game the system, who make false promises to secure parole for a fee, before the process is actually implemented. Put simply, noncitizens face a heightened risk of being victimized by immigration scammers the longer it takes to implement this process. To mitigate these risks, the President's announced process should be implemented swiftly—by August 19.

USCIS seeks emergency processing of the Form I-131F in accordance with 5 C.F.R. § 1320.13. USCIS certifies that the requirements of 5 C.F.R. § 1320.13(a) are met and that:

- The collection of information is needed immediately and is essential to the mission of the agency.
- The use of normal clearance procedures is reasonably likely to prevent or disrupt the collection of information.

USCIS greatly appreciates the timely consideration of this request.

Recommendation: DHS recommends the emergency approval of this collection of information under 5 C.F.R. § 1320.13.

¹ Exec. Order No. 14012, *Restoring Faith in Our Legal Immigration System and Strengthening Integration and Inclusion Efforts for New Americans*, 86 Fed. Reg. 8277 (Feb. 5, 2021).

**STATEMENT FOR
APPLICATION FOR PAROLE IN PLACE FOR CERTAIN NONCITIZEN SPOUSES
AND STEPCHILDREN OF U.S. CITIZENS
OMB Control No.: 1615-NEW COLLECTION INSTRUMENT(S): FORM I-131F**

A. Justification

- 1. Explain the circumstances that make the collection of information necessary.
Identify any legal or administrative requirements that necessitate the collection.
Attach a copy of the appropriate section of each statute and regulation mandating
or authorizing the collection of information.**

Section 212(d)(5) of the Immigration and Nationality Act (INA) (8 U.S.C. 1182(d)(5)) provides the Secretary of Homeland Security with the discretionary authority to parole applicants for admission into the United States “temporarily, under such conditions as the Secretary may prescribe, only on a case-by-case basis for urgent humanitarian reasons or significant public benefit.” INA sec. 212(d)(5)(A), 8 U.S.C. 1182(d)(5)(A); see also 6 U.S.C. 202(4) (charging the Secretary with the responsibility for “[e]stablishing and administering rules...governing...parole”).

On June 18, 2024, President Biden announced that the U.S. Department of Homeland Security (DHS) would implement a parole in place process for certain noncitizen spouses of U.S. citizens (and noncitizen stepchildren of U.S. citizens). Pursuant to the Secretary’s statutory authorities, including sections 103(a) and 212(d)(5)(A) of the INA, 8 U.S.C. 1103(a), 1182(d)(5)(A), the Secretary has the discretionary authority to establish a process by which certain aliens are permitted to apply for parole in place within the United States. Currently, individuals can file Form I-131, Application for Travel Document, to request certain types of parole from U.S. Citizenship and Immigration Services (USCIS). The current version of Form I-131 available for use by filers does not include an ability to specifically request parole in place. A revised version of Form I-131 was recently approved by OMB [June 17, 2024; 1615-0013], and will, for the first time, include an option for applicants to request parole in place. However, as a multi-use form that includes requests for re-entry permits, refugee travel documents, advance parole documents, and initial parole documents for individuals who are outside the United States, the Form I-131 collects limited information related to parole in place filings and does not have the data fields necessary to support the parole in place process being established for certain noncitizen spouses and stepchildren of U.S. citizens. Moreover, the revised Form I-131 is not yet available for online or paper filing.

Due to the volume of estimated respondents and the need to collect specific information and evidence that is not required for other types of parole in place requests, USCIS has created a new information collection specifically for the parole in place process for certain noncitizen spouses of U.S. citizens (and noncitizen stepchildren of U.S. citizens). Applicants filing a request for parole in place under this process would file online using

the Form I-131F, Application for Parole in Place for Certain Noncitizen Spouses and Stepchildren of U.S. Citizens.

Any individual may be required to submit biometric information if the regulations or form instructions require such information or if requested in accordance with 8 CFR 103.2(b)(9). DHS may collect and store for present or future use, or reuse, by electronic or other means, the biometric information submitted by an individual. DHS may use this biometric information to conduct background and security checks, adjudicate immigration and naturalization benefits, and perform other functions related to administering and enforcing the immigration and naturalization laws. *See* 8 CFR 103.16. Individuals requesting parole in place as the spouse or stepchild of a U.S. citizen must provide biometrics as part of the requirements for establishing eligibility.

Authorities: 8 U.S.C. 1103(a) and 1182(d)(5)(A); 6 U.S.C. 202, 271

This Emergency Revision:

In this emergency request, U.S. Citizenship and Immigration Services (USCIS) seeks approval to collect information for the purpose of considering, on a case-by-case basis, requests for parole in place from certain noncitizens who are married to a U.S. citizen (and from noncitizen stepchildren of U.S. citizens) and are present in the United States without admission or parole.

Form I-131F, Application for Parole in Place for Certain Noncitizen Spouses and Stepchildren of U.S. Citizens., will be used by noncitizens who are present in the United States without admission or parole to request a temporary period of parole in place under the Parole Process for Certain Noncitizen Spouses and Stepchildren of U.S. Citizens, announced on June 18, 2024.

DHS, in its discretion, may grant parole on a case-by-case basis for urgent humanitarian reasons or significant public benefit to any noncitizen who is an applicant for admission. This authority extends to noncitizens present in the United States who have not been lawfully admitted, a practice known as parole in place. If USCIS approves Form I-131F filed by a noncitizen seeking parole in place under this parole process, the noncitizen will receive a Form I-94, Arrival/Departure Record, which is evidence of their parole.

If granted parole in place, the noncitizen would be able to immediately apply for employment authorization as a parolee pursuant to 8 C.F.R. 274a.12(c)(11). If granted parole in place, these parolees may also become eligible to file an application to adjust their status to that of lawful permanent resident based on their relationship to their U.S. citizen spouse or stepparent. USCIS has estimated that approximately 550,000 individuals could apply for parole in place. Upon approval of an I-131F, applicants may apply for other immigration benefits once eligible.

2. **Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information**

received from the current collection.

Form I-131F will be used by certain noncitizens to request parole in place on the basis of being a qualified noncitizen spouse or stepchild of a U.S. citizen who is present in the United States without admission or parole under the Parole Process for Certain Noncitizen Spouses and Stepchildren of U.S. Citizens. USCIS will use the information collected on the form to verify the applicant's status and determine their eligibility to obtain parole in place. These requests will be considered on a case-by-case basis.

Noncitizens filing Form I-131F are required to provide biometrics and undergo background and security vetting in connection with the application. As part of the procedures for conducting these security checks, biometrics submission requirements and guidance are contained in the form instructions. USCIS retains its authority to fingerprint individuals, on an as needed, case-by-case basis. Applicants will file Form I-131F online.

- 3. Describe whether, and to what extent, the collection of information involves the use of automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of responses, and the basis for the decision for adopting this means of collection. Also describe any consideration of using information technology to reduce burden.**

This information collection provides the most efficient means for gathering and processing information for an applicant to request parole in place on the basis of being a qualified noncitizen spouse or stepchild of a U.S. citizen. The form also collects biographic information about the beneficiary to be used for biographic security screening and information concerning why the beneficiary warrants a discretionary grant of parole.

Form I-131F will only be available for online filing. The burden for setting up a USCIS online account is covered under the USCIS Online Account Access information collection (OMB control number 1615-0122).

USCIS uses various tools to collect feedback from end users of USCIS information collections. These tools include surveys or focus groups designed to collect general information, as well as public feedback submitted to USCIS either in response to an official solicitation of public comments from Federal Register publications or submitted proactively through USCIS' robust external outreach activities with stakeholders (see, e.g., www.uscis.dhs.gov/outreach). USCIS also performed usability testing on USCIS Forms I-765, N-400, and I-485 (the three forms with the highest-filing volume) with the goal of studying cross-cutting issues that impact the responding public across the entirety of the USCIS collections of information. Form I-131F is a new information collection, designed based off user feedback from USCIS Form I-134A, Online Request to be a Supporter and Declaration of Financial Support and USCIS Form I-131, Application for Travel Document. USCIS monitored the submission process of these forms, analyzed the feedback that it received from respondents, as well as input from internal assessment of

user experience to design Form I-131F.

In addition to feedback from external stakeholders, our analysis considers consultation with internal agency stakeholders regarding such activities including, but not limited to, document submission, evidentiary requirements, and like activities. USCIS extensively engages with various program, policy, and intake teams for feedback on the information collections. USCIS analyzes the results of all these efforts to identify necessary modifications to the collection tools approved for use under the Paperwork Reduction Act. Such modifications could include clarifying edits, potential question removal, and instructional updates, all intended to further support the respondent's experience in complying with a collection of information. The collection of information proposed in this current submission is the cumulative result of analysis and studies conducted. USCIS is creating this information collection to account for populations of noncitizens that will request parole in place as the spouse or stepchild of a U.S. citizen. This information collection is crucial to ensuring that the appropriate information and supporting evidence is provided by the applicant for USCIS to determine eligibility for the benefit being sought.

4. Describe efforts to identify duplication. Show specifically why any similar information already available cannot be used or modified for use for the purposes described in Item 2 above.

USCIS programs impose no duplication of efforts because similar information that can be used to determine eligibility for parole in place as the noncitizen spouse or stepchild of a U.S. citizen under Parole Process for Certain Noncitizen Spouses and Stepchildren of U.S. Citizens, online Form I-131F, is not collected through other USCIS collections or programs. USCIS requires applicants under this control number to appear at a USCIS Application Support Center (ASC) to provide an electronic photograph and fingerprints.

USCIS has also investigated the information that may be obtained from other Federal programs and agencies and has determined that the information necessary to determine if the individual is eligible to request parole in place as the noncitizen spouse or stepchild of a U.S. citizen is not available through other Federal sources.

5. If the collection of information impacts small businesses or other small entities (Item 5 of OMB Form 83-I), describe any methods used to minimize burden.

This collection of information does not have an impact on small businesses or other small entities.

6. Describe the consequence to Federal program or policy activities if the collection is not conducted or is conducted less frequently, as well as any technical or legal obstacles to reducing burden.

The collection of this information is required to verify the status of applicants who are

requesting parole in place as a qualified noncitizen spouse or stepchild of a U.S. citizen and to determine whether the applicant is eligible for a discretionary grant of parole in place. The inability of USCIS to collect information for this purpose may result in noncitizens who entered the United States without being inspected and admitted or paroled being unable to potentially adjust their status to that of a lawful permanent resident while in the United States even though they may have a qualifying relationship with a U.S. citizen. Instead, these noncitizens would have to seek an immigrant visa abroad at a U.S. consulate or embassy, and their departure from the United States can cause them to become inadmissible to the United States, requiring them to seek a waiver of that inadmissibility (if available), the process for which may be lengthy.

Alternatively, this group of noncitizens may file Form I-601A, Application for Provisional Unlawful Presence Waiver, prior to departing the United States and if Form I-601A is approved, they would have to depart the United States to seek an immigrant visa from Department of State. Even with an approved Form I-601A, such a departure could result in extended separation due to consular backlogs with significant disruption to families here in the United States, and the Form I-601A approval does not guarantee that a waiver will be granted or that the beneficiary would be able to reenter the United States after departure if other grounds of inadmissibility may apply to their case.

7. Explain any special circumstances that would cause an information collection to be conducted in a manner:

- **Requiring respondents to report information to the agency more often than quarterly;**
- **Requiring respondents to prepare a written response to a collection of information in fewer than 30 days after receipt of it;**
- **Requiring respondents to submit more than an original and two copies of any document;**
- **Requiring respondents to retain records, other than health, medical, government contract, grant-in-aid, or tax records for more than three years;**
- **In connection with a statistical survey, that is not designed to produce valid and reliable results that can be generalized to the universe of study;**
- **Requiring the use of a statistical data classification that has not been reviewed and approved by OMB;**
- **That includes a pledge of confidentiality that is not supported by authority established in statute or regulation, that is not supported by disclosure and data security policies that are consistent with the pledge, or which unnecessarily impedes sharing of data with other agencies for compatible confidential use; or**

- Requiring respondents to submit proprietary trade secret, or other confidential information unless the agency can demonstrate that it has instituted procedures to protect the information's confidentiality to the extent permitted by law.

This information collection is conducted in a manner consistent with the guidelines in 5 CFR 1320.5(d)(2).

8. If applicable, provide a copy and identify the data and page number of publication in the Federal Register of the agency's notice, required by 5 CFR 1320.8(d), soliciting comments on the information collection prior to submission to OMB. Summarize public comments received in response to that notice and describe actions taken by the agency in response to these comments. Specifically address comments received on cost and hour burden.

Describe efforts to consult with persons outside the agency to obtain their views on the availability of data, frequency of collection, the clarity of instructions and recordkeeping, disclosure, or reporting format (if any), and on the data elements to be recorded, disclosed, or reported.

Consultation with representatives of those from whom information is to be obtained or those who must compile records should occur at least once every 3 years - even if the collection of information activity is the same as in prior periods. There may be circumstances that may preclude consultation in a specific situation. These circumstances should be explained.

USCIS is seeking emergency approval under 5 CFR 1320.13 and, as such, has not yet published a notice in the Federal Register. Public comments will be solicited, and this information collection request will go through a normal Paperwork Reduction Act (PRA) approval process, including a response to all comments received from the public, no later than six months after the approval of this emergency request.

9. Explain any decision to provide any payment or gift to respondents, other than remuneration of contractors or grantees.

USCIS does not provide any payment for benefit sought.

10. Describe any assurance of confidentiality provided to respondents and the basis for the assurance in statute, regulation or agency policy.

There are no statutory or regulatory confidentiality provisions that apply to noncitizen spouses or stepchildren of U.S. citizens specifically under this parole in place process. However, DHS applies the protections of the Privacy Act of 1974, 5 U.S.C. 552a, which restricts the disclosure of personally identifiable information maintained by Federal Agencies, to all individuals as a matter of policy. Additionally, if qualifying noncitizen

spouses or stepchildren of U.S. citizens apply for other benefit types that provide special protections from disclosure or confidentiality, the statutory and regulatory provisions governing those benefit requests will apply. In particular, noncitizens who apply for asylum are protected by the confidentiality provisions of 8 CFR 208.6 and 1208.6, while applicants who have applied for T nonimmigrant status, for U nonimmigrant status, or a VAWA self-petition will be protected by the confidentiality provisions of 8 U.S.C. 1367.

This collection is covered under the following Privacy Impact Assessments:

- DHS/USCIS/PIA-056 - USCIS Electronic Information System (USCIS ELIS); and,
- DHS/USCIS/PIA-071 - myUSCIS Account Experience.

The collection is covered under the following System of Records Notices:

- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, September 18, 2017, 82 FR 43556;
- DHS/USCIS-007 Benefits Information System, October 10, 2019, 84 FR 54622; and,
- DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records, July 31, 2018, 83 FR 36950.,

11. Provide additional justification for any questions of a sensitive nature, such as sexual behavior and attitudes, religious beliefs, and other matters that are commonly considered private. This justification should include the reasons why the agency considers the questions necessary, the specific uses to be made of the information, the explanation to be given to persons from whom the information is requested, and any steps to be taken to obtain their consent.

USCIS will collect the Spouse or Parent's Social Security Number (SSN). The SSN will enable USCIS to expedite the confirmation of the U.S. citizen spouse or stepparent who is identified as the qualifying relative for purposes of the parole in place process for the noncitizen spouse or stepchild. The SSN information is used to establish and corroborate the U.S. citizen's identity, especially since not all U.S. citizens have a U.S. passport or A-number (naturalized citizens).

12. Provide estimates of the hour burden of the collection of information. The statement should:

- **Indicate the number of respondents, frequency of response, annual hour burden, and an explanation of how the burden was estimated. Unless directed to do so, agencies should not conduct special surveys to obtain information on which to base hour burden estimates. Consultation with a sample (fewer than 10) of potential respondents is desirable. If the hour burden on respondents is expected to vary widely because of differences in activity, size, or complexity, show the range of estimated hour burden, and explain the reasons for the**

variance. Generally, estimates should not include burden hours for customary and usual business practices.

- **If this request for approval covers more than one form, provide separate hour burden estimates for each form and aggregate the hour burdens in Item 13 of OMB Form 83-I.**
- **Provide estimates of annualized cost to respondents for the hour burdens for collections of information, identifying and using appropriate wage rate categories. The cost of contracting out or paying outside parties for information collection activities should not be included here. Instead, this cost should be included in Item 14.**

Type of Respondent	Form Name / Number	A	B	C (=Ax B)	D	E (=Cx D)	F	(=Ex F)
		No. of Respondents	No. of Responses per Respondent	Total Number of Responses	Avg. Burden per Response (in hours)	Total Annual Burden (in hours)	Avg. Hourly Wage Rate	Total Annual Respondent Cost
Individuals or Households	Application for Parole in Place for Certain Noncitizen Spouses and Stepchildren of U.S. Citizens, I-131F (Online e-file)	550,000	1	550,000	1.1667	641,685	\$45.96	\$29,491,843
Individuals or Households	Biometrics	550,000	1	550,000	1.17	643,500	\$45.96	\$29,575,260
Total				1,100,000		1,285,185		\$59,067,103

*The above Average Hourly Wage Rate is the [May 2023 Bureau of Labor Statistics](#) average wage for All Occupations of \$31.48 times the wage rate benefit multiplier of 1.46 (to account for benefits provided) equaling \$45.96.

** USCIS is seeking emergency approval under 5 CFR 1320.13. USCIS has estimated that as many as 550,000 individuals could apply for parole in place during the first 14 months of the process. USCIS expects this to be the totality of submission. To keep the information collection approved, USCIS will be initiate a future PRA action, reviewing the number of receipted fillings to adjust respondents at that time.

13. Provide an estimate of the total annual cost burden to respondents or record keepers resulting from the collection of information. (Do not include the cost of any hour burden shown in Items 12 and 14).

- **The cost estimate should be split into two components: (a) a total capital and start-up cost component (annualized over its expected useful life); and (b) a total operation and maintenance and purchase of services component. The estimates should take into account costs associated with generating, maintaining, and disclosing or providing the information. Include descriptions of methods used to**

estimate major cost factors including system and technology acquisition, expected useful life of capital equipment, the discount rate(s), and the time period over which costs will be incurred. Capital and start-up costs include, among other items, preparations for collecting information such as purchasing computers and software; monitoring, sampling, drilling and testing equipment; and record storage facilities.

- If cost estimates are expected to vary widely, agencies should present ranges of cost burdens and explain the reasons for the variance. The cost of purchasing or contracting out information collection services should be a part of this cost burden estimate. In developing cost burden estimates, agencies may consult with a sample of respondents (fewer than 10), utilize the 60-day pre-OMB submission public comment process and use existing economic or regulatory impact analysis associated with the rulemaking containing the information collection, as appropriate.
- Generally, estimates should not include purchases of equipment or services, or portions thereof, made: (1) prior to October 1, 1995; (2) to achieve regulatory compliance with requirements not associated with the information collection; (3) for reasons other than to provide information or keep records for the government; or (4) as part of customary and usual business or private practices.

There are no capital, start-up, operational or maintenance costs associated with this collection of information. For informational purposes only, the filing fee for Form I-131F is \$580, and applicants will file the form online.

This information collection may impose some out-of-pocket costs on respondents in addition to the time burden for the form's preparation. Costs may include payments for document translation and preparation services, attorney and legal fees, postage, and costs associated with gathering documentation. USCIS estimates that the average cost for these activities is \$515.00. The estimated out of pocket cost to respondents is 550,000 respondents multiplied by the average cost per response of \$515 = **\$283,250,000**.

14. Provide estimates of annualized cost to the Federal government. Also, provide a description of the method used to estimate cost, which should include quantification of hours, operational expenses (such as equipment, overhead, printing, and support staff), and any other expense that would not have been incurred without this collection of information. Agencies also may aggregate cost estimates from Items 12, 13, and 14 in a single table.

The estimated cost to the government, which is funded by USCIS user fee collections, is calculated by multiplying the estimated number of respondents (550,000) x the filing fee for the collection (\$580). The total cost to the Federal government is **\$319,000,000**.

15. Explain the reasons for any program changes or adjustments reporting in Items 13

or 14 of the OMB Form 83-I.

There are no program changes or adjustments as this is a new information collection.

16. For collections of information whose results will be published, outline plans for tabulation, and publication. Address any complex analytical techniques that will be used. Provide the time schedule for the entire project, including beginning and ending dates of the collection of information, completion of report, publication dates, and other actions.

This information collection will not be published for statistical purposes.

17. If seeking approval to not display the expiration date for OMB approval of the information collection, explain the reasons that display would be inappropriate.

USCIS will display the expiration date for OMB approval of this information collection.

18. Explain each exception to the certification statement identified in Item 19, "Certification for Paperwork Reduction Act Submission," of OMB 83-I.

USCIS does not request an exception to the certification of this information collection.

B. Collections of Information Employing Statistical Methods.

There is no statistical methodology involved with this collection.

USCIS Form I-131F

AUTHORITIES: USCIS is collecting the information requested on this application, and the associated evidence, under the Immigration and Nationality Act (INA) sections 103, 208(c)(1)(C), 211, 212(d)(5)(A), 215 and 8 CFR sections 211.1(a)(3-4), 212.5, and 223.1-223.3.

[Section 103 of the INA](#)

[Section 208\(c\)\(1\)\(C\) of the INA](#)

[Section 212\(d\)\(5\)\(A\) of the INA](#)

[Section 215 of the INA](#)

[8 CFR 211.1\(a\) \(3-4\)](#)

[8 CFR 212.5](#)

[8 CFR 223.1-223.3](#)



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

This form serves as the official determination by the DHS Privacy Office to identify the privacy compliance requirements for all Departmental uses of personally identifiable information (PII).

A Privacy Threshold Analysis (PTA) serves as the document used to identify information technology (IT) systems, information collections/forms, technologies, rulemakings, programs, information sharing arrangements, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer, pursuant to Section 222 of the Homeland Security Act, and to assess whether there is a need for additional Privacy Compliance Documentation. A PTA includes a general description of the IT system, information collection, form, technology, rulemaking, program, pilot project, information sharing arrangement, or other Department activity and describes what PII is collected (and from whom) and how that information is used and managed.

Please complete the attached Privacy Threshold Analysis and submit it to your component Privacy Office. After review by your component Privacy Officer the PTA is sent to the Department's Senior Director for Privacy Compliance for action. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form and assess whether any privacy compliance documentation is required. If compliance documentation is required – such as Privacy Impact Assessment (PIA), System of Records Notice (SORN), Privacy Act Statement, or Computer Matching Agreement (CMA) – the DHS Privacy Office or component Privacy Office will send you a copy of the relevant compliance template to complete and return.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis (PTA)

Specialized Template for Information Collections (IC) and Forms

The Forms-PTA is a specialized template for Information Collections and Forms. This specialized PTA must accompany all Information Collections submitted as part of the Paperwork Reduction Act process (any instrument for collection (form, survey, questionnaire, etc.) from ten or more members of the public). Components may use this PTA to assess internal, component-specific forms as well.

Form Number: **I-131F**

Form Title:	Application for Parole in Place for Certain Noncitizen Spouses and Stepchildren of U.S. Citizens		
Component:	U.S. Citizenship and Immigration Services (USCIS)	Office:	Service Center Operations Directorate (SCOPS)

IF COVERED BY THE PAPERWORK REDUCTION ACT:

Collection Title:	Form I-131F, Application for Parole in Place for Certain Noncitizen Spouses and Stepchildren of U.S. Citizens		
OMB Control Number:	1615-NEW	OMB Expiration Date:	To be determined
Collection status:	New Collection	Date of last PTA (if applicable):	Not applicable

PROJECT OR PROGRAM MANAGER

Name:	Shelly Sweeney		
Office:	Service Center Operations Directorate (SCOPS)	Title:	Adjudications Officer
Phone:	202-271-9724	Email:	Shelly.A.Sweeney@uscis.dhs.gov

COMPONENT INFORMATION COLLECTION/FORMS CONTACT



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
 202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

Name:	James Perry		
Office:	Regulatory Coordination Division – Paperwork Reduction Act Branch	Title:	Project Manager
Phone:	301-416-9873	Email:	James.T.PerryJr@uscis.dhs.g ov

SPECIFIC IC/Forms PTA QUESTIONS

1. Purpose of the Information Collection or Form

a. Describe the purpose of the information collection or form. *Please provide a general description of the project and its purpose, including how it supports the DHS mission, in a way a non-technical person could understand (you may use information from the Supporting Statement).*
If this is an updated PTA, please specifically describe what changes or upgrades are triggering the update to this PTA.

USCIS is submitting this updated PTA to document the addition of three data elements to the form titled Form I-131F, Application for Parole in Place for Certain Noncitizen Spouses and Stepchildren of U.S. Citizens. The form is currently in the process of being reviewed and approved by the Office of Management and Budget (OMB). The addition of the Spouse or Parent's full name, date of birth, and, if available, Social Security Number (SSN) will enable USCIS to expedite the confirmation of the U.S. citizen spouse or stepparent who is identified as the qualifying relative for purposes of the parole in place process for the noncitizen spouse or stepchild. The SSN information is used to establish and corroborate the U.S. citizen's identity, especially since not all U.S. citizens have a U.S. passport or A-number (naturalized citizens).

The Form I-131F, Application for Parole in Place for Certain Noncitizen Spouses and Stepchildren of U.S. Citizens, will be used by noncitizens who are present in the United States without admission or parole to request a temporary period of parole in place under INA section 212(d)(5)(A) under the new Process to Promote the Unity and Stability of Families.

DHS, in its discretion, may grant parole on a case-by-case basis for urgent humanitarian reasons or significant public benefit to any noncitizen who is an applicant for admission. This authority extends to noncitizens present in the United States who have not been lawfully admitted, a practice known as "parole in place." If USCIS approves the Form I-131F filed for a noncitizen seeking parole in place, the noncitizen will receive a Form I-94, Arrival/Departure Record, which is evidence of their parole. NOTE: Form I-94 does not authorize entry into the United States after departure. Individuals granted parole



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
 202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

under this process who depart the United States without first obtaining an Advance Parole Document may be unable to return and/or barred from eligibility for future immigration benefits, including adjustment of status to that of lawful permanent resident (Green Card).

USCIS is in the process of creating and implementing a parole in place (PIP) process for certain noncitizen spouses and stepchildren of U.S. citizens who are present in the United States without admission or parole. Under this process, noncitizens who are married to U.S. citizens, who have not been inspected and admitted or paroled, who have been continuously physically present in the United States for at least ten years as of June 17, 2024, and who meet certain other requirements, may be considered for parole in place on a case-by-case basis for urgent humanitarian reasons or significant public benefit. The process for this particularized population to apply and be considered for parole in place on a case-by-case basis will achieve the significant public benefit of promoting the unity and stability of American families, increasing the economic prosperity of American communities, strengthening diplomatic relationships with partner countries in the region, reducing strain on limited U.S. government resources, and furthering national security and public safety objectives. Certain noncitizen children of a U.S. citizen may also request parole in place under this process, provided that they are physically present in the United States without admission or parole as of June 17, 2024 and meet the Immigration and Nationality Act's definition and requirements of a stepchild of a U.S. citizen.

A separate Form I-131F must be filed for each noncitizen seeking parole in place under the Unity and Stability of Families parole process. Upon receipt of a properly filed parole in place request, USCIS will determine on a case-by-case basis whether a grant of parole is warranted based on a significant public benefit or urgent humanitarian reasons and whether the applicant merits a favorable exercise of discretion. All requests will take into consideration the potential requestor's previous immigration history, criminal history, the results of background checks and national security and public safety vetting, and any other relevant information available to or requested by USCIS.

If paroled, these noncitizens will generally be able to apply for lawful permanent residence without having to leave the United States and be processed by a U.S. consulate overseas. DHS estimates that 500,000 noncitizen spouses of U.S. citizens could be eligible to access this process; on average, these noncitizens have resided in the United States for 23 years. Approximately 50,000 noncitizen children of these spouses are estimated to be eligible to seek parole under this process.

A noncitizen may request parole in place under this process if they:

- (1) Are present in the United States without admission or parole;



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
 202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

(2) Have been continuously physically present in the United States:

- (a) Since at least June 17, 2014, if seeking parole in place as the spouse of a U.S. citizen OR
- (b) As of June 17, 2024, if seeking parole in place as the stepchild of a U.S. citizen;

(3) Have:

- (a) A legally valid marriage to a U.S. citizen on or before June 17, 2024, if seeking parole in place as the spouse of a U.S. citizen OR
- (b) A parent who had a legally valid marriage to a U.S. citizen on or before June 17, 2024, and before the stepchild's 18th birthday, if seeking parole in place as the stepchild of a U.S. citizen;

(4) Do not have any disqualifying criminal history; and

(5) Do not pose a threat to national security and public safety.

Even if an individual meets the above criteria allowing them to seek a discretionary grant of parole under this process, USCIS may deny the request if it is determined that a grant of parole is not warranted in the specific individual's case.

Relevant Information Technology

Individuals must submit the Form I-131F electronically. Online filing for the Form I-131F is available via myUSCIS, a customer service tool that provides an online public-facing portal for USCIS customers to access information related to their applications, petitions, and service requests. Individuals may use their myUSCIS online account to electronically file Form I-131F once authenticated. All supporting evidence for the Form I-131F may also be submitted to in electronic form via their myUSCIS online account.

After an applicant properly submits Form I-131F with the correct fee and signature, information from the form is ingested into the USCIS Electronic Information System (USCIS ELIS) system, an internal case management system used by USCIS officers to review and adjudicate cases. USCIS ELIS will receive the electronic filing directly from myUSCIS after ingestion. The Form I-131F and any supporting evidence are then routed to an officer for adjudication. The officer updates USCIS ELIS with an adjudicative decision, and a notice of that decision (a request for evidence, notice of intent to deny, approval, or denial) is issued to the applicant.



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
 202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

<p>b. List the DHS (or Component) authorities to collect, store, and use this information. <i>If this information will be stored and used by a specific DHS component, list the component-specific authorities.</i></p> <p>The primary legal authority supporting the collection of information derives from 8 USC sections 1103, 1158, 1181, 1182(d)(5), 1185, 1225, and 1229b(b)(4); 6 USC section 202(4); and 8 CFR sections 211.1(a), 212.5, 223.1-223.3, and 235.1-235.5.</p>
--

2. Describe the IC/Form

<p>a. Does this form collect any Personally Identifiable Information" (PII¹)?</p>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<p>b. From which type(s) of individuals does this form collect information? <i>(Check all that apply.)</i></p>	<input checked="" type="checkbox"/> Members of the public <input type="checkbox"/> U.S. citizens or lawful permanent residents <input checked="" type="checkbox"/> Non-U.S. Persons <input type="checkbox"/> DHS Employees/Contractors (list Components) <input type="checkbox"/> Other federal employees or contractors
<p>c. Who will complete and submit this form? <i>(Check all that apply.)</i></p>	<input checked="" type="checkbox"/> The record subject of the form (e.g., the individual applicant). <input checked="" type="checkbox"/> Legal Representative (preparer, attorney, etc.). <input type="checkbox"/> Business entity. <p>If a business entity, is the only information collected business contact information?</p> <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Law enforcement.

¹ Personally identifiable information means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
 202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

	<input type="checkbox"/> DHS employee/contractor. <input type="checkbox"/> Other individual/entity/organization that is NOT the record subject. <i>Please describe.</i> Click here to enter text.
d. How do individuals complete the form? <i>Check all that apply.</i>	<input type="checkbox"/> Paper. <input checked="" type="checkbox"/> Electronic. (ex: fillable PDF) <input type="checkbox"/> Online web form. (available and submitted via the internet) <i>Provide link:</i>
e. What information will DHS collect on the form? <i>List all individual PII data elements on the form. If the form will collect information from more than one type of individual, please break down list of data elements collected by type of individual.</i>	
<p><u>Data collected from aliens if an alien is filing the form:</u></p> <ul style="list-style-type: none"> • Selection of either 1) Spouse of a United States Citizen; or 2) Stepchild of a United States Citizen • Spouse or Parent's I-131F Receipt Number (if applicable) • Spouse or Parent's full name • Spouse or Parent's date of birth • Spouse or Parent's Social Security Number (SSN) (if any) • First, middle and last name • Other first, middle, and last names (if applicable) • Current U.S. Mailing address (street number and name, city/town, state, and ZIP code) • Current U.S. Physical address (street number and name, city/town, state, and ZIP code) • U.S. Safe address (street number and name, city/town, state, and ZIP code), if applicable • Alien Registration Number (A-Number) (if any) • Country of birth • Country of citizenship or nationality • Gender • Date of birth • Marital Status 	



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
 202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

- Date of marriage, if applicable
- U.S. Social Security number (if any)
- USCIS Online Account Number (if any)
- Most recent Form I-94 Arrival/Departure Record Number (if any)
- Ethnicity (Select from: Hispanic or Latino; Not Hispanic or Latino)
- Race (Select from: American Indian or Alaska Native; Asian; Black or African American; Native Hawaiian or Other Pacific Islander; White)
- Height
- Weight
- Eye color
- Hair color
- Daytime phone number
- Mobile phone number
- Email address
- Processing Information
 - Date You Began Your Continuous Physical Presence in the United States (mm/dd/yyyy)
 - Have you EVER been in any exclusion, deportation, removal, or rescission proceedings?
 - Have you EVER been arrested for, charged with, or convicted of a felony or misdemeanor, including incidents handled in juvenile court, in the United States? Do not include minor traffic violations unless they were alcohol or drug-related.
 - Have you EVER been arrested for, charged with, or convicted of a crime in any country other than the United States?
 - Have you EVER or are you NOW engaged in activities that could be reasonable grounds for concluding that you are a danger to public safety or to the security of the United States?
 - If you have ever filed a Form I-601A, Application for a Provisional Unlawful Presence Waiver, with USCIS, provide the receipt number: [receipt number field]
 - Explain how you qualify for parole in place, including information regarding the significant public benefit or urgent humanitarian reasons warranting a grant of parole, and why you believe you merit a favorable exercise of discretion. Upload copies of any supporting documents or evidence you wish considered. [Free text field]
- Evidence of your relative's status as a U.S. Citizen such as a copy of their US birth certificate, naturalization certificate, certificate of citizenship, Consular Report of Birth Abroad, or a US passport



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
 202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

- Evidence of qualifying relationship such as a marriage certificate, birth certificate, or death certificate
- Evidence of continuous physical presence such as documents stating date of entry into the US, deeds/mortgages/rent receipts, utility bills, vehicle registrations, tax returns, school records, records from a religious entity in the United States confirming your participation in a religious ceremony, rite, or passage (e.g., baptism, first communion, wedding), etc.
- Evidence of disposition of any criminal record
- Evidence demonstrating the significant public benefit or urgent humanitarian reasons warranting a grant of parole and evidence of any additional favorable discretionary factors that you would like USCIS to consider
- Signature
- Date of Signature

Data collected from interpreters if an interpreter is used:

- First and last name
- Interpreter's business or organization name
- Daytime phone number
- Mobile phone number (if any)
- Email address (if any)
- Signature
- Date of Signature

Data collected from preparers if a preparer is used:

- First and last name
- Preparer's business or organization name
- Daytime phone number
- Mobile phone number (if any)
- Email address (if any)
- Signature
- Date of Signature

f. Does this form collect Social Security number (SSN) or other element that is stand-alone Sensitive Personally Identifiable Information (SPII)? *Check all that apply.*

Social Security number

DHS Electronic Data Interchange

Alien Number (A-Number)

Personal Identifier (EDIPI)

Tax Identification Number

Social Media Handle/ID



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
 202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

<input type="checkbox"/> Visa Number	<input type="checkbox"/> Known Traveler Number
<input type="checkbox"/> Passport Number	<input type="checkbox"/> Trusted Traveler Number (Global
<input type="checkbox"/> Bank Account, Credit Card, or other	Entry, Pre-Check, etc.)
financial account number	<input type="checkbox"/> Driver's License Number
<input checked="" type="checkbox"/> Other. <i>Please list:</i> Form I-94	<input type="checkbox"/> Biometrics
Arrival/Departure Record Number	

g. List the **specific authority** to collect SSN or these other SPII elements.

INA 264(f) (8 USC 1304(f)), states, "Alien's social security account number. Notwithstanding any other provision of law, the Attorney General is authorized to require any alien to provide the alien's social security account number for purposes of inclusion in any record of the alien maintained by the Attorney General or the Service."

8 CFR 103.2(b)(9) provides that USCIS "may require any applicant, petitioner, sponsor, beneficiary, or individual filing a benefit request, or any group or class of such persons submitting requests, to appear for an interview and/or biometric collection."

h. How will the SSN and SPII information be used? What is the purpose of the collection?

The purpose of the collection is to assist USCIS in determining the individual's identity and eligibility for the benefit being sought.

Further, USCIS seeks to collect the spouse or parent's SSN to facilitate and expedite the confirmation of the U.S. citizen spouse or stepparent who is identified as the qualifying relative for purposes of the parole in place process for the noncitizen spouse or stepchild. The SSN information is used to establish and corroborate the U.S. citizen's identity, especially since not all U.S. citizens have a U.S. passport or A-number (naturalized citizens). The SSN will also allow DHS to perform additional vetting critical in our efforts to make sure the parole in place process is not used to facilitate human trafficking or other transnational criminal activity. DHS will use this SSN to query the holdings of interagency and intelligence community partners, and as needed, to query state, local, or international agencies. Additionally, the SSN provides a unique identifier to link online filings. Inclusion of this data element will allow DHS to quickly identify, through systematic checks, trends, and other indicators in the filings of spouses and stepchildren of U.S. citizens that may reveal patterns commonly associated with human trafficking and transnational criminal activity. This data element will provide DHS additional tools to identify potential cases that require further investigation decisioning



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
 202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

on the form or for which DHS may initiate an interview with a U.S. citizen spouse to confirm the bona fides of the marriage.

i. Is SSN necessary to carry out the functions of this form and/or fulfill requirements of the information collection? *Note:* even if you are properly authorized to collect SSNs, you are required to use an alternative identifier. If there are technological, legal, or regulatory limitations to eliminating the SSN, privacy-enhancing alternatives should be taken, such as truncating the SSN.

SSNs are used strictly to determine a person's identity. The authority to collect information in Global is set forth in the Immigration and Nationality Act, 8 U.S.C. §§ 1103, 1225, 1228, 1304, et seq., Title II of Public Law 105-100, and in the implementing, regulations found in volume 8 of the Code of Federal Regulations (CFR).

<p>j. Are individuals provided notice at the time of collection by DHS (<i>Does the records subject have notice of the collection or is form filled out by third party?</i>)?</p>	<p><input checked="" type="checkbox"/> Yes. Please describe how notice is provided. USCIS provides a Privacy Notice to the individual on the Form I-131F instructions prior to collecting any information.</p> <p><input type="checkbox"/> No.</p>
---	--

3. How will DHS store the IC/form responses?

<p>a. How will DHS store the original, completed IC/forms?</p>	<p><input type="checkbox"/> Paper. Please describe.</p> <p><input checked="" type="checkbox"/> Electronic. Please describe the IT system that will store the data from the form.</p> <p>The Form I-131F may be filed online via myAccount Experience. Information is then ingested into USCIS ELIS for review and adjudication.</p> <p><input type="checkbox"/> Scanned forms (completed forms are scanned into an electronic repository). Please describe the electronic repository.</p>
--	---



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
 202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

<p>b. If electronic, how does DHS input the responses into the IT system?</p>	<p><input type="checkbox"/> Manually (data elements manually entered). Please describe.</p> <p><input checked="" type="checkbox"/> Automatically. Please describe.</p> <p>The Form I-131F may be filed online via myAccount Experience. Information is then ingested into USCIS ELIS for review and adjudication.</p>
<p>c. How would a user search the information submitted on the forms, <i>i.e.</i>, how is the information retrieved?</p>	<p><input checked="" type="checkbox"/> By a unique identifier.² <i>Please describe.</i> If information is retrieved by personal identifier, please submit a Privacy Act Statement with this PTA.</p> <p>Information may be retrieved by Receipt number, Social Security number, Alien Registration Number, name, date of birth, or a combination of name and date of birth.</p> <p><input type="checkbox"/> By a non-personal identifier. <i>Please describe.</i> Click here to enter text.</p>
<p>d. What is the records retention schedule(s)? <i>Include the records schedule number.</i></p>	<p>USCIS ELIS: All benefit request forms and other electronic records in USCIS ELIS are designated as A-File records. A-File records are permanent, whether hard copy or electronic. DHS transfers A-Files to NARA for retention for 100 years after the individual's date of birth. [N1-566-08-011]</p>
<p>e. How do you ensure that records are disposed of or deleted in accordance with the retention schedule?</p>	<p>The record owner is responsible for ensuring the records are deleted in accordance with a retention schedule. Record owners review their respective repositories annually and adhere to the associated records retention schedule transfer and/or deletion guidance.</p>

² Generally, a unique identifier is considered any type of “personally identifiable information,” meaning any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

f. Is any of this information shared outside of the original program/office? *If yes, describe where (other offices or DHS components or external entities) and why. What are the authorities of the receiving party?*

Yes, information is shared with other DHS components or offices. Please describe.

The information from the form may be shared to DHS ICE and DHS CBP via system access.

Yes, information is shared *external* to DHS with other federal agencies, state/local partners, international partners, or non-governmental entities. Please describe.

No. Information on this form is not shared outside of the collecting office.



Please include a copy of the referenced form and Privacy Act Statement (if applicable) with this PTA upon submission.



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
 202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	Shannon DiMartino
Date submitted to Component Privacy Office:	August 8, 2024
Concurrence from other Components involved (if applicable):	Click here to enter text.
Date submitted to DHS Privacy Office:	August 8, 2024
Have you approved a Privacy Act Statement for this form? (Only applicable if you have received a waiver from the DHS Chief Privacy Officer to approve component Privacy Act Statements.)	<input checked="" type="checkbox"/> Yes. Please include it with this PTA submission. <input type="checkbox"/> No. Please describe why not. Click here to enter text.
<p>Component Privacy Office Recommendation:</p> <p><i>Please include recommendation below, including what existing privacy compliance documentation is available or new privacy compliance documentation is needed.</i></p> <p>USCIS is submitting this updated PTA to document the addition of three data elements to the form titled Form I-131F, Application for Parole in Place for Certain Noncitizen Spouses and Stepchildren of U.S. Citizens. The form is currently in the process of being reviewed and approved by the Office of Management and Budget (OMB). The addition of the Spouse or Parent's full name, date of birth, and, if available, Social Security Number (SSN) will enable USCIS to expedite the confirmation of the U.S. citizen spouse or stepparent who is identified as the qualifying relative for purposes of the parole in place process for the noncitizen spouse or stepchild. The SSN information is used to establish and corroborate the U.S. citizen's identity, especially since not all U.S. citizens have a U.S. passport or A-number (naturalized citizens).</p> <p>The Form I-131F, Application for Parole in Place for Certain Noncitizen Spouses and Stepchildren of U.S. Citizens, will be used by noncitizens who are present in the United States without admission or parole to request a temporary period of parole in place under INA section 212(d)(5)(A) under the new Process to Promote the Unity and Stability of Families.</p>	



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

The USCIS Office of Privacy recommendation is to designate Form I-131F as privacy sensitive with coverage under the following compliance documentation:

PIAs

- DHS/USCIS/PIA-056 USCIS Electronic Immigration System (USCIS ELIS), which covers adjudicative actions pertaining to the Form I-131F.
- DHS/USCIS/PIA-071 myUSCIS Account Experience, which covers the electronic submission of forms to USCIS, including Form I-131F.

SORNs

- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, which covers the physical and electronic immigration files, including A-Files and Receipt Files.
- DHS/USCIS-007 Benefits Information System, which covers the collection, use and storage of data elements USCIS collects about benefit requestors, beneficiaries, legal representatives, interpreters, and preparers to process the Form I-131F.
- DHS/USCIS-018 Immigration Biometric and Background Check, which covers the background checks that are performed in association with ELIS.



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ADJUDICATION

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	Portia Johnson
PCTS Workflow Number:	0017776
Date approved by DHS Privacy Office:	August 8, 2024
PTA Expiration Date	August 8, 2027
DHS Privacy Office Approver (if applicable):	Schuntel Reddock

DESIGNATION

Privacy Sensitive IC or Form:	Yes If "no" PTA adjudication is complete.
Determination:	<input type="checkbox"/> PTA sufficient at this time. <input type="checkbox"/> Privacy compliance documentation determination in progress. <input type="checkbox"/> New information sharing arrangement is required. <input type="checkbox"/> DHS Policy for Computer-Readable Extracts Containing SPII applies. <input checked="" type="checkbox"/> Privacy Act Statement required. <input checked="" type="checkbox"/> Privacy Impact Assessment (PIA) required. <input checked="" type="checkbox"/> System of Records Notice (SORN) required. <input type="checkbox"/> Specialized training required. <input type="checkbox"/> Other. Click here to enter text.
Privacy Act Statement:	e(3) statement currently accurate. PN has been submitted and approved.
System PTA:	No system PTA required. Click here to enter text.
PIA:	System covered by existing PIA If covered by existing PIA, please list: <ul style="list-style-type: none"> • DHS/USCIS/PIA-056 USCIS Electronic Immigration System (USCIS ELIS) • DHS/USCIS/PIA-071 myUSCIS Account Experience If a PIA update is required, please list: Click here to enter text.



Homeland Security

Privacy Office
 U.S. Department of Homeland Security
 Washington, DC 20528
 202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

SORN:	<p>System covered by existing SORN</p> <p>If covered by existing SORN, please list:</p> <ul style="list-style-type: none"> • DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, September 18, 2017, 82 FR 43556 • DHS/USCIS-007 Benefits Information System, October 10, 2019, 84 FR 54622 • DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records, July 31, 2018, 83 FR 36950 <p>If a SORN update is required, please list: Click here to enter text.</p>
DHS Privacy Office Comments: <i>Please describe rationale for privacy compliance determination above.</i>	

USCIS submitted this updated PTA to document the addition of three data elements to the form titled Form I-131F, Application for Parole in Place for Certain Noncitizen Spouses and Stepchildren of U.S. Citizens. The form is currently in the process of being reviewed and approved by the Office of Management and Budget (OMB). The addition of the Spouse or Parent's full name, date of birth, and, if available, Social Security Number (SSN) will enable USCIS to expedite the confirmation of the U.S. citizen spouse or stepparent who is identified as the qualifying relative for purposes of the parole in place process for the noncitizen spouse or stepchild. The SSN information is used to establish and corroborate the U.S. citizen's identity, especially since not all U.S. citizens have a U.S. passport or A-number (naturalized citizens). The Form I-131F, Application for Parole in Place for Certain Noncitizen Spouses and Stepchildren of U.S. Citizens, will be used by noncitizens who are present in the United States without admission or parole to request a temporary period of parole in place under INA section 212(d)(5)(A) under the new Process to Promote the Unity and Stability of Families.

DHS, in its discretion, may grant parole on a case-by-case basis for urgent humanitarian reasons or significant public benefit to any noncitizen who is an applicant for admission. This authority extends to noncitizens present in the United States who have not been lawfully admitted, a practice known as "parole in place." If USCIS approves the Form I-131F filed for a noncitizen seeking parole in place, the noncitizen will receive a Form I-94, Arrival/Departure Record, which is evidence of their parole. NOTE: Form I-94 does not authorize entry into the United States after departure. Individuals granted parole under this process who depart the United States without first obtaining an Advance Parole Document may be unable to return and/or barred from eligibility for future immigration benefits, including adjustment of status to that of lawful permanent resident (Green Card).



Homeland Security

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

DHS PRIV agrees that this is a privacy-sensitive form because it collects PII and SPII from members of the public. PRIV recommends coverage under DHS/USCIS/PIA-056 USCIS Electronic Immigration System (USCIS ELIS), which covers adjudicative actions pertaining to the Form I-131F; and DHS/USCIS/PIA-071 myUSCIS Account Experience, which covers the electronic submission of forms to USCIS, including Form I-131F.

SORN coverage is required because data is being retrieved by a unique identifier. SORN coverage is provided under DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, which covers the physical and electronic immigration files, including A-Files and Receipt Files; DHS/USCIS-007 Benefits Information System, which covers the collection, use and storage of data elements USCIS collects about benefit requestors, beneficiaries, legal representatives, interpreters, and preparers to process the Form I-131F; and DHS/USCIS-018 Immigration Biometric and Background Check, which covers the background checks that are performed in association with ELIS.



Privacy Impact Assessment
for the

USCIS Electronic Immigration System (USCIS ELIS)

DHS/USCIS/PIA-056(a)

December 3, 2018

Contact Point
Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
(202) 272-8030

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717



Abstract

U.S. Citizenship and Immigration Services (USCIS) operates the USCIS Electronic Immigration System (USCIS ELIS). USCIS ELIS was originally developed to serve as a public-facing electronic filing system supporting the submission of benefit request forms. USCIS ELIS also served as the internal case management system for USCIS adjudicators to efficiently process benefit request forms. USCIS ELIS was recently redesigned to exclusively serve as an internal electronic case management system for electronically filed benefit request forms and certain paper forms. MyUSCIS Account Experience replaced all aspects of the public-facing USCIS ELIS.¹ USCIS is updating and reissuing the USCIS ELIS PIA to discuss the shift from supporting the public-facing electronic filing system to serving solely as an internal case management system with new functionalities and system interconnections. This PIA replaces the previously issued DHS/USCIS/PIA-056 published on May 17, 2016. As USCIS ELIS adds other forms and services, USCIS will update this PIA and its appendices accordingly.

Overview

USCIS is the component within the Department of Homeland Security (DHS) that oversees lawful immigration to the United States. In part, the USCIS mission is to provide accurate information while ensuring the integrity of the U.S. immigration system and adjudicating requests efficiently and fairly. USCIS receives applications, petitions, and other benefit requests (collectively referred to as *benefit request forms*) from individuals seeking immigration and non-immigration benefits. USCIS has historically received paper-based applications for adjudication and relied on a complex paper-based process to execute the immigration and naturalization mission.

USCIS is continuing the current paper-based operations and also steadily transforming to an electronic, online environment to improve operational efficiency, and improve customer engagement. Currently, most benefit request forms, including all supporting evidence, are still submitted in paper format by applicants, petitioners, or requestors (collectively referred to as *benefit requestors*), or their legal representatives. In turn, USCIS communicates case information and issues paper notices to benefit requestors and legal representatives.

USCIS offers an alternate filing method, online filing, to improve the way benefit requestors and legal representatives apply for and manage immigration benefit requests by shifting the process from a paper-based system to a secure online case management system. The MyUSCIS Account Experience offers a personalized, online account for benefit requestors and legal

¹ See DHS/USCIS/PIA-071 MyUSCIS Account Experience, available at www.dhs.gov/privacy.



representatives to electronically file benefit request forms, and replaces all aspects of the public-facing electronic filing component previously available through USCIS ELIS.

Since the MyUSCIS Account Experience is now the public-facing online filing component, USCIS ELIS serves as the primary internal case management system for both electronically filed and paper-based benefit request forms. USCIS ELIS creates person-centric accounts for each benefit requestor. USCIS will continue to expand available immigration product lines within USCIS ELIS to support the agency's modernization initiative of receiving and processing forms in an electronic environment.

Application Initiation

As described in the Benefit Request and Intake PIA, to begin the benefit request process, the benefit requestor must complete a USCIS benefit request form.² Individuals have the option to complete the benefit request form either by paper or, if available, electronically, through an online account. Both methods collect the same information and fees. Upon completion, individuals submit the benefit request form, required supporting documents and filing fee payment, or fee waiver request, as appropriate. Individuals submit benefit request forms according to the form instructions. USCIS ELIS receives paper forms through the USCIS Lockbox facilities³ or electronically from a system interconnection with MyUSCIS.⁴

Paper Filings

USCIS requires benefit requestors to submit paper benefit request forms to a specified Lockbox facility. U.S. Lockbox facilities are operated by the U.S. Department of Treasury (Treasury) and are staffed by financial agents working on behalf of USCIS to receive paper requests, process payments, and forward the immigration requests as directed by USCIS for further processing. This contractor manages the intake of paper USCIS benefit request forms and the collection of associated fees submitted by mail. The Lockbox operates the mechanisms to convert the submitted information into an electronic format, deposit associated filing fees, generate a receipt or rejection notices to applicants, and transmit the benefit request information to the USCIS ELIS system. The contractor does not approve or deny benefit request forms received by the USCIS Lockbox. The Lockbox scans an image of the benefit request form and supporting documentation into an electronic format and sends it to USCIS ELIS for ingestion. Depending on the form type, after the form is ingested into USCIS ELIS, the paper copy may be destroyed.

Once information from the paper filing is received, USCIS ELIS generates a "USCIS Account Acceptance Notice" and mails the notice through the U.S. Postal Service (USPS) to the

² See DHS/USCIS/PIA-061 Benefit Request and Intake Process, available at www.dhs.gov/privacy.

³ The USCIS Lockbox serves as a collection receptacle for the intake of forms and processing of fees for immigration benefit request forms. For more information, see www.uscis.gov/lockbox.

⁴ See DHS/USCIS/PIA-071 MyUSCIS Account Experience, available at www.dhs.gov/privacy.



Homeland Security

Privacy Impact Assessment DHS/USCIS/PIA-056(a) USCIS ELIS Page 3

benefit requestor and legal representative, when applicable. This notice contains instructions for creating an optional USCIS online account and contains a passcode which, if used, can link the submitted paper submission into the newly created online account.⁵ By creating this online account, a benefit requestor who filed paper benefit request forms has the opportunity to log into his or her MyUSCIS online account to access his or her case information. Online account capabilities include the ability to check the personalized processing status of the submitted benefit request, obtain copies of USCIS-issued documents associated with the filing (i.e., appointment notices and request for evidence), and respond electronically to requests for additional information, such as Requests for Evidence (RFE).

As a security measure, the passcode sent in the “USCIS Account Acceptance Notice” expires in 30 days. The benefit requestor, however, may later contact the USCIS National Customer Service Center (NCSC) to request the generation of a new “USCIS Account Acceptance Notice” with a new activation passcode.⁶ Benefit requestors who choose not to activate their online accounts can continue engaging with USCIS through the existing paper-based process.

Online Filing

Benefit requestors who electronically file their request use the MyUSCIS Account Experience, which offers a personalized, authenticated, and secured account for benefit requestors and legal representatives to file benefit forms. MyUSCIS Account Experience replaces all aspects of the public-facing USCIS ELIS. Through MyUSCIS Account Experience, benefit requestors and/or legal representatives are able to create a personal profile, securely and electronically file benefit request forms, access pending case information, and securely communicate with USCIS personnel.

The electronic filing component of MyUSCIS Account Experience offers an interactive tool that assists individuals with completing certain immigration benefit request forms or certain fee payments. The electronic benefit request forms collect the same information as the corresponding paper forms. To initiate the benefit request completion process, the individual selects his or her desired form type and enters valid data into all required fields. The account holder may save, edit, delete, or update information when the form is in draft state. MyUSCIS Account Experience does not keep copies of previous draft iterations and deletes cases if inactive for 30 days. Prior to the submission of the benefit request form, the account holder has the opportunity to review the provided information.

After preparing a benefit request, the individual or his or her representative submits the benefit request form by electronically signing the form and providing payment directly to the

⁵ See DHS/USCIS/PIA-071 MyUSCIS Account Experience, available at www.dhs.gov/privacy.

⁶ See DHS/USCIS/PIA-054 National Customer Service Center, available at www.dhs.gov/privacy.



Department of Treasury through an embedded pay.gov screen.⁷ MyUSCIS sends the filing to USCIS ELIS for processing once the payment is accepted. USCIS ELIS has a direct interface with MyUSCIS Account Experience. While there is no public-facing component of USCIS ELIS, it continues to serve as an internal electronic case management system that allows USCIS adjudicators to process benefit requests.

Benefit Request Lifecycle

USCIS ELIS is a person-centric case management system used to track and adjudicate certain benefit request forms. Once a benefit request form is submitted to USCIS, a series of processing and adjudication actions occur, such as case receipt and intake, biometric collection appointment generation, case specific processing and management, automated background check, interview appointment scheduling, final decision rendering, and production of the proof of benefit.

USCIS benefit request forms generally undergo the following steps: (1) Case Intake; (2) General Pre-Adjudication Procedures (i.e., identity validation checks); (3) Security Screening Checks; (4) Case Processing; (5) Interview; (6) Decision Rendering; and (7) Post-Adjudication Processing. USCIS ELIS supports each of these tasks. For each step in the process, USCIS ELIS sends case status updates with the latest case status to MyUSCIS Account Experience and Case Status Online to provide the benefit requestor with the latest status of their benefit filing.⁸

Initial Intake

Case Creation

Benefit request submissions consist of the specific request forms and supporting documentation and may originate in an electronic format or be converted to an electronic format from paper. Upon receipt of a benefit request, USCIS ELIS ingests and stores the benefit request forms and supplemental evidence submitted through the USCIS Lockbox or MyUSCIS online account and creates a person-centric case for the benefit request filing. USCIS ELIS then searches, identifies, and consolidates all previous cases associated with the individual within the system to present to the adjudicator in a singular and comprehensive view. USCIS ELIS provides information on the individual's identity, immigration status, previous immigration benefits processed in USCIS ELIS, and details and results of previous background identity and security checks.

⁷ Payment information is collected by the Department of Treasury's Pay.gov system (see Financial Management Service (FMS) PIA and Revenue Collection Records – Treasury/FMS.017 SORN, 68 FR 5691

⁸ See DHS/USCIS/PIA-019 Customer Relationship Interface System (CRIS), available at www.dhs.gov/privacy.



When a new case is created, USCIS ELIS interfaces with RAILS (not an acronym)⁹ to annotate the applicable Alien File¹⁰ content residing in USCIS ELIS. RAILS is an automated file-tracking system used to maintain an accurate file inventory and track the physical and electronic location of immigration files.¹¹ Alien File content in USCIS ELIS may originate in an electronic format or have been converted to an electronic format from paper. All benefit request forms, supporting evidence submitted with a benefit request, and system data generated for the case are electronically maintained in USCIS ELIS as part of the Alien File and serve as part of the official agency record.

General Pre-Adjudication Procedures

Alien Number Validation

USCIS ELIS then validates the benefit requestor's Alien Number (A-Number), if applicable, as the first step of the adjudication process. When benefit requestors list an A-Number on a benefit request, USCIS ELIS concurrently¹² runs an automated comparison of the provided A-Number against the USCIS Central Index System 2 (CIS 2)¹³ and Alien Number Validation Microservice.¹⁴ CIS employs a strict, Boolean matching process to the data to determine if there is a match or no match.¹⁵ The A-Number Validation Microservice employs a fuzzy match search to find a list of candidate matches that account for common errors such as keyboard distance typing errors, transposition of letters or numbers, and transliteration of foreign names.¹⁶ The candidate

⁹ RAILS is the modernized update to the National File Tracking System. See DHS/USCIS/PIA-032 National File Tracking System (NFTS) and associated updates, available at www.dhs.gov/privacy.

¹⁰ The Alien File, or A-File, is created for aliens seeking immigration benefits (i.e., lawful permanent resident, naturalization), aliens who illegally entered the United States, or other individuals subject to the provisions of the Immigration and Nationality Act (INA).

¹¹ The purpose of the A-File is to record an individual's immigration applications, petitions, and requests, as well as enforcement transactions as he or she interacts with the U.S. immigration system. The content in the A-Files consist of paper and electronic records of the individual's immigration transactions, which may include records of immigration benefit requests, requests for agency action, and adjudication outcomes.

¹² Currently, USCIS is running two A-number validation services. USCIS continues to evaluate use of the A-Number Validation Microservice against the CIS results. This comparison serves to identify any output errors and refine the algorithms used by the microservice to increase the accuracy of this automated A-Number validation tool when it will serve as the primary A-Number Validation system.

¹³ See DHS/USCIS/PIA-009(a) Central Index System, available at www.dhs.gov/privacy.

¹⁴ See forthcoming DHS/USCIS/PIA-00# Person Centric Identity Management (PCIM), available at www.dhs.gov/privacy.

¹⁵ Boolean Logic is a form of algebra that is centered around three simple words known as Boolean Operators: "Or," "And," and "Not." At the heart of Boolean Logic is the idea that all values are either true or false. The use of Boolean Logic allows for the creation of more complex audience definitions, allowing for audiences to be built to a very specific set of definitions.

¹⁶ Fuzzy matching is a method that provides an improved ability to process word-based matching queries to find matching phrases or sentences from a database. When an exact match is not found for a sentence or phrase, fuzzy matching can be applied. Fuzzy matching attempts to find a match which, although not a 100 percent match, is above the threshold matching percentage set by the application. Fuzzy matching is mainly used in computer-assisted translation and other related applications.



matches are then scored using a statistical algorithm to determine the confidence score of how likely the candidate match is the correct match.

USCIS ELIS runs the two automated comparisons of the applicant declared A-Number against CIS and Alien Number Validation Microservice search results to verify that the A-Number: (1) exists and is valid, and (2) matches the name and other biographic identifying information (i.e., date of birth, country of birth, country of citizenship/nationality, and A-Number) provided by the individual. These A-Number Validation tools apply the respective matching logic to validate A-numbers provided by individuals filing benefit requests against the primary A-Number on record for the individual in various USCIS systems, as well as generate a computed confidence score for the match. The computed score is a percentage of confidence based on matching fields and characters. Based on thresholds established for these scores, cases either pass or fail the automated A-Number validation process. The declared A-Number must be an exact match with CIS for the A-Number Validation microservice to return a success message and for the case to continue to USCIS ELIS processing with no manual intervention. If the system cannot automatically verify this information, USCIS ELIS moves the benefit requestor's request into an electronic work queue in which the A-Number discrepancy is researched and resolved by a USCIS adjudicator before proceeding to adjudication.

Screening (Background, Identity, and Security Checks)

Biometric Collections

After the A-Number is validated, USCIS ELIS interfaces with the National Appointment Scheduling Service (NASS)¹⁷ to schedule an Application Support Center (ASC) biometric collection appointment for the benefit requestor, a requirement for certain requests. USCIS requires benefit requestors and beneficiaries for certain immigration benefits to submit their biometrics along with biographic information provided in the benefit request to USCIS for background, identity, and security checks.

USCIS uses NASS to schedule biometric appointments for the collection of fingerprints, photographs, and signatures at an ASC. Each scheduling request sent to NASS includes the benefit requestor's name, address, and benefit type. NASS uses the information from USCIS ELIS to schedule a biometric appointment at the ASC location closest to the benefit requestor address of record. Once scheduled, NASS sends a biometric appointment confirmation notice for generation and printing to the Enterprise Print Manager Service (EPMS) and Notice Generation System (NGS).¹⁸ Once the notice is generated, a copy of the notice is stored in USCIS ELIS. EPMS

¹⁷ See DHS/USCIS/PIA-057 National Appointment Scheduling System, available at www.dhs.gov/privacy.

¹⁸ EPMS and NGS are legacy systems that were specifically developed for notice generation and printing purposes. NGS only generates notices and EPMS prints the notices and mails these notices directly to the individuals. EPMS supports the printing of notices, cards, and booklets for USCIS. For additional information see DHS/USCIS/PIA-063 Benefit Decision and Output Processes, available at www.dhs.gov/privacy.



Homeland Security

Privacy Impact Assessment DHS/USCIS/PIA-056(a) USCIS ELIS Page 7

generates a physical appointment notice that is mailed to the benefit requestor and the legal representative.

At the biometric appointment, USCIS electronically captures the benefit requestor's fingerprints and declared biographic information that is required to verify the individual's identity and ensure that the correct biographic information is associated with the captured biometrics. This data is associated together and stored in Customer Profile Management System (CPMS), which is the centralized source of biometric images used for USCIS benefit card and document production.¹⁹

For benefit fillings that require biometric collections, the case in USCIS ELIS cannot move to the next stage in the process until the ASC appointment is completed, and the ASC Notification message is sent to USCIS ELIS, confirming that the applicant appeared at the ASC and biometrics were collected. USCIS is then able to electronically provide various notices of agency action (e.g., interview appointment notices, requests for evidence or originals, notices of intent to deny, or final agency decisions) for a specific case directly to the benefit requestor or legal representative through his or her MyUSCIS online account. Individuals who do not have an online account can continue to receive notices from USCIS through the mail.

Background, Identity, and Security Checks

Most individuals submitting benefit request forms are subject to background, identity, and security checks to ensure eligibility for the requested benefit and to ensure that they do not pose a threat to public safety or to the national security of the United States. USCIS conducts background, identity, and security checks as part of case processing.

USCIS runs fraud, criminal, and national security background checks against the following systems:

- **U.S. Customs and Border Protection (CBP) TECS (not an acronym) Name Check:**²⁰ USCIS conducts a mandatory TECS check on all applicants, petitioners, and beneficiaries. TECS is an automated enforcement and inspection lookout system that combines information from multiple agencies, databases, and system interfaces to compile data relating to national security risks, public safety issues, current or past targets of investigations, and other law enforcement concerns. The system is maintained by CBP, and is the principal system used by officers at the border to assist with screening and determinations regarding admissibility of arriving persons. USCIS

¹⁹ See DHS/USCIS/PIA-060 Customer Profile Management Service, available at www.dhs.gov/privacy.

²⁰ See DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing, available at www.dhs.gov/privacy.



Homeland Security

Fraud Detection and National Security (FDNS) Directorate uses the ATLAS System²¹ to facilitate the required TECS checks when performing name checks for all cases processed in USCIS ELIS. The database searches against the Automated Biometric Identification System (IDENT),²² Federal Bureau of Investigation (FBI) National Crime Information Center (NCIC), and Terrorist Screening Database.²³ ATLAS provides alerts to FDNS and USCIS Background Check Officers indicating information that may have an impact on the processing of the petition or application and may need to be resolved. Information from a case may also be sent to CBP's Advanced Targeting System²⁴ as part of a Continuous Immigration Vetting (CIV) process. These checks are facilitated using the ATLAS system. Results are stored in the FDNS Data System (FDNS-DS)²⁵ and made available to USCIS ELIS.

- **FBI Fingerprint Check:**²⁶ USCIS ELIS sends 10 fingerprints and related biographic data to the FBI Next Generation Identification System (NGI) for a criminal background check. USCIS ELIS receives the FBI criminal background check response (i.e., “Non-Match” or “Match”).
- **FBI Name Check:**²⁷ USCIS ELIS sends name, date of birth, country of birth, and other biographic data to the FBI Name Check Program. The FBI Name Check is performed as a part of the National Name Check Program (NNCP). USCIS ELIS receives responses for the FBI Name Check request. The results will generally indicate whether the benefit seeker has any pertinent or derogatory information.
- **Biometric Identity Check:**²⁸ USCIS ELIS queries DHS Office of Biometric Identity Management (OBIM) Automated Biometric Identification System (IDENT) for biometric identity verification and to conduct background checks. The information sent to IDENT includes 10 fingerprints, photo, and biographic information. IDENT creates

²¹ See DHS/USCIS/PIA-013-01 Fraud Detection and National Security Directorate, available at www.dhs.gov/privacy.

²² The Automated Biometric Identification System (IDENT) is the central DHS-wide system for storage and processing of biometric and associated biographic information for national security; law enforcement; immigration and border management; intelligence; background investigations for national security positions and certain positions of public trust; and associated testing, training, management reporting, planning and analysis, or other administrative uses. See DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), available at www.dhs.gov/privacy.

²³ See DHS/ALL/PIA-027 DHS Watchlist Service, available at www.dhs.gov/privacy.

²⁴ See DHS/CBP/PIA-006 Automated Targeting System, available at www.dhs.gov/privacy.

²⁵ See DHS-USCIS-PIA-013(a) Fraud Detection and National Security Data System (FDNS-DS), available at www.dhs.gov/privacy.

²⁶ See DOJ/FBI Next Generation Identification System PIA available at www.fbi.gov/services/records-management/foipa/privacy-impact-assessments.

²⁷ See DOJ/FBI Name Check PIA available at www.fbi.gov/services/records-management/foipa/privacy-impact-assessments.

²⁸ See DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), available at www.dhs.gov/privacy.



a new encounter with a unique Encounter Identification Number (EID), which is a unique number found in the Identity Verification Tool (IVT)²⁹ along with Fingerprint Identification Number (FIN).³⁰ IDENT provides information related to previous encounters stored in IDENT. The information from these encounters will be used in the adjudication process.

- **Port of Entry Check:**³¹ USCIS ELIS queries DHS CBP Arrival and Departure Information System (ADIS) for date of entry and port of entry.
- **Criminal History Check:**³² USCIS ELIS queries DHS ICE Enforcement Integrated Database (EID) for background information related to the requestor. USCIS ELIS queries EID for information related to the arrest, booking, detention, and removal of persons encountered during immigration and law enforcement investigations and operations conducted by ICE and CBP. EID is a DHS shared common database repository for several DHS law enforcement and homeland security applications.

If the fraud, criminal, and national security background check identifies potential criminal, public safety, or national security concerns, the matter is referred to another electronic workflow queue within USCIS ELIS for resolution. USCIS takes specific measures to address and resolve the presented concerns before adjudicating the benefit request, which may include a referral to the USCIS FDNS Directorate.

Case Processing

If biometrics are not required, the benefit requestor's case advances to the adjudication step immediately following A-Number validation and resolution of any background check results. If biometrics are required, the benefit requestor's case advances once USCIS CPMS sends notification that the benefit requestor has submitted his or her biometrics at the ASC. USCIS ELIS automatically places the benefit request in an adjudicator work queue after A-Number validation, completion of the biometric collections and background checks, and return of the background and security check results have occurred.

The USCIS adjudicator evaluates all data—the information submitted by the benefit requestor along with the results of the background and security checks—according to existing standard operating procedures (SOP) that apply to the benefit request form. USCIS adjudicators may need to review the A-File (if available) to verify the identity and benefit eligibility of the benefit requestor. Adjudicators are able to view some A-File content in USCIS ELIS. If an adjudicator requires a physical A-File, the adjudicator can request the file in USCIS ELIS using a

²⁹ IVT provides the capability to compare an individual's biometric and biographic information to previous biometric encounters captured by other agencies within OBIM IDENT.

³⁰ When a biometric is submitted to the OBIM IDENT for an individual and it is his or her first enrollment in IDENT, a unique identifier is assigned—the Fingerprint Identification Number (FIN).

³¹ See DHS/CBP/PIA-024 Arrival and Departure Information System (ADIS) available at www.dhs.gov/privacy.

³² See DHS/ICE/PIA-015 Enforcement Integrated Database (EID), available at www.dhs.gov/privacy.



Homeland Security

Privacy Impact Assessment

DHS/USCIS/PIA-056(a) USCIS ELIS
Page 10

direct interface with RAILS. USCIS ELIS sends the following to RAILS: full name, the primary tracking number (the alien number (A-Number)), and date of birth. RAILS collects the following information from USCIS ELIS: adjudicator's full name, office location, responsible party code (RPC), which relates to either a system user or file shelf location and the immigration file's status (i.e., retired, record-in-use), and the last transaction (i.e., charged-out, received, in-transit).

To assist the adjudicator in verifying information submitted by the requestor, USCIS ELIS displays information pulled the Person-Centric Query Service (PCQS).³³ This information includes other names, biographic information, contact information, other A-Numbers, and additional immigration history data that may also be associated with the requestor. Following existing SOPs, the adjudicator is able to identify which data is correct or relevant and make updates to USCIS ELIS to record the correct data about the benefit requestor. USCIS ELIS documents all updates made to data about the requestor.

USCIS also requires supporting documentation (submitted by the requestor) as initial evidence of a benefit requestor's eligibility for a benefit. The burden of proof in establishing eligibility for an immigration benefit rests with the benefit requestor. Each benefit request form includes specific evidential requirements. When a benefit requestor can establish that certain primary evidence is unavailable, secondary evidence, also in specific forms, may be provided. Examples of supporting documentation include: copies of civil documents such as birth, marriage, or adoption certificates; divorce decrees; affidavits of financial support; criminal records; and school records.

USCIS may issue a Request for Evidence (RFE)³⁴ or Notice of Intent to Deny (NOID)³⁵ if a benefit requestor or beneficiary fails to submit evidence or provides insufficient evidence to establish eligibility. USCIS personnel use Enterprise Correspondence Handling Online (ECHO)³⁶ to generate editable notices using templates and standard text such as RFEs and NOIDs. USCIS ELIS sends the applicant's name and address to ECHO to create the notices. USCIS ELIS receives confirmation from ECHO of the notice generation and a PDF copy of the notice is stored in USCIS ELIS.

USCIS mails the notices through the U.S. Postal Service to the benefit requestor and/or her or his representative with instructions on how to respond or appropriate next steps. For benefit

³³ See DHS/USCIS/PIA-010 Person Centric Query Service (PCQS), available at www.dhs.gov/privacy.

³⁴ USCIS uses an RFE when an application lacks required documentation or the adjudicator needs additional evidence to determine an applicant's eligibility for the benefit sought. The request will indicate what evidence or information USCIS needs to fully evaluate the application or petition under review.

³⁵ A NOID is a formal statement from USCIS that it has determined that the applicant is ineligible for the immigrant benefit requested. There are a number of circumstances that may lead to a NOID being sent, and the issuance of a NOID is required when derogatory information is uncovered during the course of the adjudication that is not known to the individual, according to 8 CFR § 103.2(b)(16). Regardless of the reason behind the NOID, USCIS will grant the applicant an opportunity to overcome this determination and demonstrate that he or she is eligible.

³⁶ See DHS/USCIS/PIA-063 Benefit Decision and Output Processes, available at www.dhs.gov/privacy.



requestors with a USCIS online account, USCIS also uploads notices for storage and retrieval from their MyUSCIS online account. When a case has a representative of record, USCIS ELIS also sends the notice to the legal representative MyUSCIS online account.

Interview

A benefit requestor may be required to appear for an interview at a USCIS Field Office. To schedule an initial interview, USCIS ELIS interfaces with NASS and sends name, address, A-Number, form type, and date/time for the interview appointment. NASS sends the Interview Notice request to EPMS and NGS where the notices are generated and sent on to printing. A copy of the notice is sent back to USCIS ELIS and stored. For benefit requestors with a USCIS online account, USCIS also uploads notices into MyUSCIS online account. When a case has a representative of record, USCIS ELIS also sends the notice to the legal representative MyUSCIS online account.

All individuals who arrive at a USCIS Field Office for an interview are compared to a previously captured photograph and two-print fingerprints using a tool called Identity Verification Tool (IVT).³⁷ IVT allows USCIS Field Offices to compare an individual's biometric (fingerprint and photograph) and biographic information to information previously captured at an ASC, ensuring that the person who appeared at the ASC is the same person appearing at the USCIS Field Office.

Before the start of the interview, USCIS Field Officers may choose to record the interview, and will then notify benefit requestors that the interview may be recorded and USCIS adjudicators may use web cameras to digitally record immigration interviews.³⁸ The recordings are temporarily recorded on a workstation and then converted onto an encrypted digital optical disc storage (i.e., DVD). Once copied, the recordings are permanently erased from the workstation. The digital disc with recorded immigration interviews is then stored in the related A-File.

During in-person interviews for cases in USCIS ELIS only, USCIS adjudicators may use a tablet. At the time of such interaction, USCIS adjudicators may corroborate information declared by the requestor on a USCIS-issued form (e.g., spelling of a name), collect new information and data (e.g., signature), and collect and verify responses provided by the individual at the time of the in-person interaction. The tablet is physically connected to and communicates directly with USCIS ELIS through a USCIS computer. The tablet presents USCIS ELIS information allowing the benefit requestor to:

³⁷ See DHS/USCIS/PIA-060 Customer Profile Management System, available at www.dhs.gov/privacy.

³⁸ 8 C.F.R. § 335.2 (c) states that USCIS officers conducting an examination of the applicant for naturalization may have a videotaped transcript of the interview made, and the applicant and the Agency shall have the right to present such documentary evidence as may be required for a full and true disclosure of the facts. The recordings provide a complete record of the proceedings, which, in certain instances, may lead to enhanced detection of fraud and national security issues.



- Review biographical information;
- Review and verify any changes to information on the submitted USCIS form;
- Provide responses to any questions related to the in-person interview;
- Provide a digital or electronic signature when required; and
- Certify that reviewed revisions or changes to the information on the USCIS form are true and correct.

The USCIS adjudicator follows current processes to verify the identity of individuals at an in-person interview or examination. Any individual participating in an in-person interaction with USCIS may have his or her identity verified pursuant to the current process. The tablet may also be used to capture and record the officer's and applicant's required signatures that are stored in USCIS ELIS.

Decision Rendering

After all the steps discussed above are complete, USCIS personnel make a final determination on the benefit request. USCIS personnel may grant, deny, rescind, or revoke an immigration benefit.³⁹ Case decision actions are tracked and recorded in USCIS ELIS.

Post-Adjudication Processing

If a final decision of approval is reached by the adjudicating officer, USCIS ELIS uses automated interfaces with existing USCIS IT systems to generate the proof of benefit (such as a Lawful Permanent Resident card), as applicable. When a proof of benefit must be produced, and it requires a photograph, the adjudicator is able to obtain the requestor's facial photograph, fingerprint, and signature via an interface with CPMS solely for proof of benefit production purposes. The facial photograph and other biometric elements are temporarily displayed in USCIS ELIS and can be adjusted to improve image quality for printing. USCIS ELIS allows the user to zoom, pan, lighten, or darken the photo for card production and then certify for printing. After successful proof of benefit production is completed, the facial photograph obtained from CPMS is automatically deleted from USCIS ELIS, and the final adjusted image is stored as part of the printed card record in CPMS.

³⁹ These processes are carried out outside USCIS ELIS. For more information see DHS/USCIS/PIA-062 Administrative Appeals Office Case Management System, available at www.dhs.gov/privacy.



Post-Decision Reporting

USCIS uses the information contained in USCIS ELIS to generate a number of statistical reports to measure and evaluate workload for proper resource allocation. USCIS ELIS interfaces with the Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR) for reporting, statistical analysis, and adjudicatory purposes.⁴⁰ eCISCOR interconnects with other systems like the Standard Management Analysis and Reporting Tool (SMART) sub-system to create customizable reports.⁴¹ SMART uses USCIS ELIS data to generate reports to identify pending cases and to measure productivity trends and average processing times. USCIS also generates granular level reports to identify types, number, and status of cases located in a particular office or assigned to a particular USCIS staff member, which allows supervisors to identify the oldest cases in queue for processing.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The primary legal authority supporting the collection of the information provided to USCIS is the Immigration Nationality Act (INA).⁴² Specifically, 8 U.S.C. § 1360 requires a central file of information for the security and enforcement agencies of the Government of the United States that contains the names of all aliens admitted or denied admission to the United States and such other relevant information as required to aid in the proper enforcement of this chapter. The Homeland Security Act of 2002⁴³ and the INA charge the Secretary of Homeland Security with administration and enforcement of the immigration and naturalization laws. The Secretary of Homeland Security has delegated duties to USCIS pursuant to DHS Delegation 0150.1. DHS also has promulgated regulations that permit the collection and processing of applications, petitions, and requests online entitled, “Immigration Benefits Business Transformation, Increment I;”⁴⁴ and “Immigration Benefits Business Transformation, Increment I; Correction.”⁴⁵

⁴⁰ See DHS/USCIS/PIA-023(a) Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR), available at www.dhs.gov/privacy.

⁴¹ See DHS/USCIS/PIA-050 Standard Management Analysis Reporting Tool (SMART), available at www.dhs.gov/privacy.

⁴² 8 U.S.C. § 1101 (2004) *et seq.*

⁴³ Pub. L. No.107-296, 116 Stat. 2135 (2002), 6 U.S.C. § 112.

⁴⁴ 76 FR 53764 (Aug. 29, 2011).

⁴⁵ 76 FR 73475, (Nov. 29, 2011).



1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The following SORNs cover the collection, maintenance, and use of the information contained in USCIS ELIS:

- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records⁴⁶ covers individuals who petition for benefits under the INA, and includes petitioners, preparers, and attorneys. Information covered includes A-number, name, address, phone number, email address, Social Security number (SSN), date of birth (DOB), place of birth (POB), countries of citizenship, family history, employment history, and marriage certificates.
- DHS/USCIS-007 Benefits Information System⁴⁷ covers individuals who have filed applications or petitions for immigration benefits under INA and provides coverage for information collected such as name, SSN, records regarding tax payment and financial matters, and records regarding employment.
- DHS/USCIS-018 Immigration Biometric and Background Check⁴⁸ covers the background checks that are performed.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. The USCIS ELIS Security Plan was last updated on December 26, 2017. USCIS ELIS has been granted an authority to operate (ATO) under the USCIS Ongoing Authorization (OA) process. OA requires USCIS ELIS to be reviewed on a monthly basis and to maintain its security and privacy posture in order to retain its ATO.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

USCIS ELIS serves as the electronic record used to facilitate and track the adjudication of certain benefit requests. USCIS has many retention schedules to cover different types of data in USCIS ELIS, including the A-File, draft and filed forms, and systems.

⁴⁶ DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (Sept. 18, 2017).

⁴⁷ DHS/USCIS-007 Benefits Information System, 81 FR 72069 (Oct. 19, 2016).

⁴⁸ DHS/USCIS-018 Immigration Biometric and Background Check, 83 FR 36950 (July 31, 2018).



Electronic Records

An individual's immigration history may be in the following formats: (1) A paper A-File; (2) an electronic record in the Enterprise Document Management System (EDMS) or USCIS Electronic Immigration System; or (3) a combination of paper and electronic records and supporting documentation. USCIS ELIS maintains certain filed benefit requests with USCIS. All documentation submitted or created in support of a USCIS benefit request case is maintained in accordance with USCIS policy and NARA retention schedules after being scanned into USCIS ELIS. Benefit request forms that were rejected because the form was incomplete and/or not accompanied by the required signature or fee are maintained for 6 years or less.⁴⁹ These records have temporary value because they have little or no research value. All other benefit request forms and other electronic records in USCIS ELIS are designated as A-File records. A-File records are permanent, whether hard copy or electronic. These records have permanent value because they document enduring legal rights and have high potential research value. DHS transfers A-Files to the custody of NARA for retention for 100 years after the individual's date of birth.

USCIS ELIS Case Management

ELIS also serves as the case processing, adjudication, and management platform for certain paper and electronically filed benefit request forms. The case management and adjudication data in USCIS ELIS is covered by the retention schedule for each form type. USCIS will update Appendix A to this PIA for each form retention schedules.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Each form processed by USCIS ELIS has an existing OMB control number that covers the USCIS ELIS collection. An updated list is available in Appendix B of this PIA.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

USCIS ELIS collects:

- Information that is required to adjudicate specific benefit requests will vary for each immigration benefit type. A full account of what data is requested for each immigration

⁴⁹ Please see Appendix A to view the approved NARA schedules for form types processed in USCIS ELIS.



Homeland Security

Privacy Impact Assessment
 DHS/USCIS/PIA-056(a) USCIS ELIS
 Page 16

benefit type can be viewed by referencing the paper forms associated with each immigration benefit type in Appendix B. A comprehensive list of USCIS forms and the respective form instructions are available at www.uscis.gov/forms. USCIS ELIS also contains information from other USCIS, DHS, and external systems. USCIS ELIS information includes:

- Full name;
- Aliases;
- Mailing and physical address;
- A-Number;
- SSN (if applicable);
- USCIS Online Account Number;
- Date of birth (DOB);
- Country of birth (COB);
- Immigration status;
- Date permanent resident status became effective;
- Telephone numbers;
- Email address;
- Gender;
- Weight;
- Height;
- Eye color;
- Travel history, as reported by the applicant;
- Education history;
- Employment information; and
- Criminal history information.
- E-signature from the requestor, which includes check-box attestation, requestor's name, Internet Protocol (IP) address from which the filing is submitted, and time/date stamp;
- Background and security check results about the requestor;



- Images of the benefit request form and supplemental evidence;⁵⁰
- Case processing information and generated data, such as notices, internal case processing notes, and decisions;
- Social media handles and aliases, associated identifiable information, and publicly available search results; and
- Temporarily stored biometric images, including fingerprints and signature (if not waived), to allow proper formatting for printing.

2.2 What are the sources of the information and how is the information collected for the project?

Information within USCIS ELIS is obtained from the following sources: (1) benefit requestors, beneficiaries, accredited representatives, attorneys, form preparers, and/or interpreters, (2) internal DHS systems, and (3) external systems or sources. Most of the information in USCIS ELIS is obtained from the data provided by the benefit requestor or beneficiary on the completed benefit request form and submitted supporting documentation accompanying his or her benefit request. USCIS ELIS also interconnects with internal or external systems, and USCIS adjudicators can manually enter information into USCIS ELIS (i.e., interview comments and background dates). Most background check results are maintained in USCIS ELIS.

USCIS also collects information from publicly available sources, such as general internet searches of publicly available information including publicly available social media information. Benefit adjudicators may conduct general internet searches to verify the identity and claim of the individual. FDNS conducts social media searches to verify information provided by the requestor to investigate indications of fraudulent behavior and identify any threat to public safety or nexus to known or suspected terrorists during the processing of the requestor's benefit request. The results of the general and social media searches are used to verify information relating to the benefit request, information indicating potential fraud (such as identity fraud or document fraud), or information regarding criminal activity or national security concerns that would impact eligibility and admissibility.⁵¹ USCIS may only look at publicly available information, and will respect individuals' privacy settings. In compliance with DHS Directive 110-01, *Privacy Policy for Operational Use of Social Media and Instruction 110-01-001*,⁵² authorized FDNS personnel are

⁵⁰ Many USCIS forms require the submission of supplemental forms to establish eligibility for the benefit. Examples of supplemental evidence may include, but are not limited to, marriage certificates, birth certificates, tax records, court records, appeals and motions, personal narratives, and affidavits and sworn statements (of benefit requestors and qualifying witnesses) including details of victimization, criminal records, and terrorist engagement. The supplemental information is stored in the A-File.

⁵¹ Information collected from social media, by itself, will not be a basis to deny an immigration benefit request.

⁵² See DHS Directive 110-01, Privacy Policy for Operational Use of Social Media and Instruction 110-01-001,



Homeland Security

Privacy Impact Assessment DHS/USCIS/PIA-056(a) USCIS ELIS Page 18

permitted to access social media sites when conducting background checks or administrative investigations only after they have completed initial USCIS Privacy Requirements for the Operational Use of Social Media training and program-specific training on the authorized use of social media, and have signed the “Rules of Behavior” form.⁵³ Authorized USCIS personnel must complete refresher training and sign the Rules of Behavior annually. When social media is collected on a benefit requestor the records become part of the USCIS ELIS adjudication and are retained for the life of the benefit request form as A-File content.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Yes. USCIS ELIS maintains publicly available data from general internet searches used as part of the benefit adjudication process by adjudicators, and social media postings⁵⁴ that are used by authorized FDNS personnel trained to conduct social media reviews. FDNS uses social media postings to verify information provided by the requestor to investigate indications of fraudulent behavior and identify any threat to public safety or nexus to known or suspected terrorists in the processing of the requestor’s benefit request. The social media postings collected on a benefit requestor become part of the USCIS ELIS adjudication and are retained for the life of the benefit request form as A-File content.

USCIS only collects social media information that is reasonably related to matters under USCIS consideration. Social media may be part of the background check process for certain immigration benefit requests, and background checks are run by USCIS only where USCIS has the legal authority to do so. This policy permits specifically trained USCIS officers to access publicly available social media as an aid in determining whether an individual is eligible for an immigration benefit.

2.4 Discuss how accuracy of the data is ensured.

USCIS ELIS ensures data accuracy primarily by using data entered directly by the requestor whenever possible. All requests filed using the USCIS online accounts are completed directly by the benefit requestor except for those accounts set up by a legal representative. Benefit

available at <https://www.dhs.gov/policy>. This Directive sets privacy policy and requirements for DHS and its components for the access, collection, use, maintenance, retention, disclosure, deletion, and destruction of PII in relation to operational use of social media.

⁵³ Select USCIS personnel who seek to access, process, store, receive, or transmit PII obtained through the Operational Use of Social Media while conducting investigations or background checks are required to complete a Rules of Behavior (ROB) for the Operational Use of Social Media. These ROBs ensure that users are accountable for their actions on social media, are properly trained, and aware of the authorized use of social media sites.

⁵⁴ Privacy update regarding social media use can be found at <https://www.uscis.gov/about-us/directories-and-program-offices/privacy-updates>.



requestors are able to correct any information in their benefit request forms up to the point that they sign and submit the filing. After the benefit request has been submitted, the only changes the benefit requestor may make are at the account level, such as updating an email address or other contact information. When inputting data from a paper filing, the Lockbox facilities employ quality control measures, including levels of review to prevent keying errors and verifying scan quality. In general, in the event of an error, the requestor is able to correct certain data using existing correction processes, such as contacting USCIS NCSC.

Select data submitted by requestors are run through the A-Number validation process to promote data integrity between USCIS ELIS and CIS. Information is validated from other systems as needed. USCIS ELIS also enables the adjudicator to check biographical data (e.g., name, date of birth, place of birth, gender) against data from CIS to assist the adjudicator in identifying inaccurate data supplied by the requestor or correcting inaccurate data on file in legacy systems. Finally, USCIS automatically submits data to other federal, DHS, and USCIS systems to verify identity and conduct background and security checks.

USCIS only collects and uses external sources and publicly available information that is reasonably related to matters under USCIS consideration. No decisions are based solely on the collection of external information, including social media information. USCIS gives individuals opportunities during and after the completion of the application process to correct information they have provided and to respond to information received from external sources. If the information could lead to a denial of the immigration benefit and if it is information of which the applicant is unaware, it would be provided to the applicant in a Notice of Intent to Deny, in an interview, or in similar processes, and the applicant would have an opportunity to review and respond.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that requestors could submit more information than necessary because USCIS ELIS houses multiple benefit requests that each require different information.

Mitigation: USCIS ELIS collects information pertaining to one benefit request at a time so the requestor cannot be prompted to enter information unless it pertains to the specific benefit request for which the requestor is filing. The information collected for benefit requests is the same for paper and electronic filings.

Privacy Risk: There is a risk of over-collection of information for making a benefit determination.

Mitigation: The USCIS Office of Privacy reviews each immigration form during the form development process and/or promulgation process to ensure that only the minimum amount of information is collected to determine benefit eligibility. Furthermore, all data elements collected



are negotiated with and approved by Office of Management and Budget during PRA collection review. USCIS designed USCIS ELIS specifically to collect and store only the information that is necessary to adjudicate the benefit request forms processed by USCIS. USCIS requires the information collected and stored in USCIS ELIS to establish the identity of the benefit requestor or beneficiary and to process the benefit request to determine benefit eligibility.

Privacy Risk: There is a risk that information received from external sources could be inaccurate, resulting in a denial of benefits.

Mitigation: This risk is mitigated. USCIS gives individuals opportunities during and after the completion of the application process to correct information they have provided or received, and to respond to information received from external sources. If the information could lead to a denial of the immigration benefit and if it is information of which the benefit requestor is unaware, it would be provided to the applicant in a NOID, in an interview, or in similar processes, and the applicant would have an opportunity to review and respond.

Privacy Risk: There is a risk USCIS may rely on inaccurate information coming from social media to make a decision.

Mitigation: This risk is partially mitigated. Information is collected directly from benefit requesters, and individuals generally have some degree of control over what is posted on their social media account. USCIS presumes some of this information is accurate. During the interview, the officer will review any social media assessments provided by FDNS, including those with possible inaccurate information, and address the underlying eligibility concern as annotated on the social media assessment with the applicant and elicit testimony as indicated. FDNS has also indicated that officers may provide the applicant with an opportunity to view the social media post (the post only, not the entire social media assessment) and provide additional testimony explaining any postings. Information collected from social media, by itself, will not be a basis to deny benefit requests. USCIS has also developed procedures and training focused on understanding data quality limitations associated with social media.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

USCIS ELIS is an electronic case management system that stores information to support the processing of benefit request forms. USCIS uses the information to fulfill the following adjudicative actions:

- Verify the identity of the requester;
- Identify missing information and make requests for additional information;



- Provide a repository of data to assist with future immigration benefit requests;
- Schedule interview and biometrics appointments;
- Facilitate and maintain security screening check results to determine suitability for immigration benefits using criminal, immigration, or terrorism-related history;
- Generate and issue notices;
- Provide data necessary to assist in the determination of immigration and employment status to support the Verification Program;
- Manage adjudicative workflow;
- Share information with internal and external partners for mission-related activities; and
- Generate reports.

Submissions to USCIS ELIS may originate in an electronic format or be converted to an electronic format from paper and may include forms and supporting documentation associated with each submission. This includes notices of agency action (e.g., appointment notices, requests for evidence or originals, notices of intent to deny, or other final agency decisions) on a specific application, petition, or request, whether filed directly online or received by USCIS in a paper format and subsequently scanned for integration into the USCIS ELIS.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

USCIS ELIS shares read-only information with the USCIS Enterprise Service Bus (ESB),⁵⁵ which may share information from USCIS ELIS with other components via PCQS.⁵⁶ Through PCQS, USCIS provides U.S. Immigration and Customs Enforcement (ICE) and CBP read-only access to ELIS data. Both agencies are within DHS and share immigration-related missions.

⁵⁵ See DHS/USCIS/PIA-008 Enterprise Service Bus available at www.dhs.gov/privacy.

⁵⁶ See DHS/USCIS/PIA-010 Person Centric Query System (PCQS) available at www.dhs.gov/privacy.



3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that retaining records in electronic, rather than paper, format will allow increased access to the information.

Mitigation: This risk is partially mitigated. USCIS mitigates this risk three ways. First, all users of USCIS ELIS must receive role-based system training, which explains the purpose of the data and includes reminders about proper PII handling. Second, the system tracks all access and edits to requestor PII and stores that activity in back-end audit logs available to the USCIS Office of Security Investigations for monitoring and action. Finally, USCIS ELIS employs a provisioning process that verifies that every user requesting access to the system has a valid need to view data in the system.

Privacy Risk: By retaining data in an active, online platform, USCIS ELIS poses a risk of unauthorized exposure because the system could be attacked by an external entity.

Mitigation: USCIS recognizes that retaining data online makes that data potentially more available to compromise. As a result, USCIS is building into its retention schedules a timeframe after which data may be retained offline by the agency but not online with public access. This will allow the agency to preserve records that should be maintained for their historical value but adds some security from unauthorized access of outdated accounts because the information is behind the firewall. This risk is also mitigated by IT security measures such as encryption of data in transit and at rest and requiring secure two-factor authentication for login. The USCIS OA process supports a near real-time review and evaluation of system vulnerabilities and risks and provides a framework to support risk management decisions. Both the USCIS Office of Information Technology and USCIS ELIS systems teams report any incidents to the DHS Emergency Operations Center. USCIS also follows National Institute of Standards and Technology (NIST) guidance SP 800-63-3 (Digital Identity Guidelines) and SP 800-63A (Enrollment and Identity Proofing) to authenticate an individual's identity to ensure data is accessed only by authorized individuals.⁵⁷

Privacy Risk: By creating an electronic immigration file in addition to the paper file, USCIS ELIS poses a risk of further decentralizing the official file of a requestor and making the record incomplete and inaccurate.

Mitigation: This is partially mitigated. USCIS recognizes that retaining data online and on paper creates a risk for USCIS officials when receiving immigration requests. In the RAILS there is a “flag” if a USCIS ELIS case with a paper file exists. This provides awareness that the A-file content may exist in both paper and electronic formats. RAILS is an enterprise wide application

⁵⁷ National Institute of Standards and Technology, U.S. Department of Commerce, NIST Special Publication 800-63A Digital Identity Guidelines, Enrollment and Identity Proofing Requirements. June 2017. <https://pages.nist.gov/800-63-3/sp800-63a.html>.



that supports the USCIS mission to maintain control of alien/immigrant and receipt files. The purpose of RAILS is to increase the ability of USCIS to track the movement of Alien/immigrant and Receipt physical files.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Each benefit request form, regardless of whether it is paper or electronic, contains a Privacy Notice that provides notice to individuals about the collection, USCIS's authority to collect information, the purposes of data collection, routine uses of the information, and the consequences of declining to provide the requested information to USCIS. The forms also contain a provision by which an applicant authorizes USCIS to release any information received from the benefit requestor or beneficiary as needed to determine eligibility for benefits. Additionally, individuals receive general notice through this PIA, DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking SORN, DHS/USCIS-018 Immigration Biometric and Background Check SORN, and the DHS/USCIS-007 Benefits Information System SORN.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

By submitting benefit request forms to USCIS, benefit requestors have consented to USCIS's use of the information submitted for adjudication purposes. Applicants who apply for USCIS benefits have an opportunity and ability to decline to provide information. USCIS benefit request forms require the benefit requestor to provide biographic and/or biometric information. This information is critical in making an informed adjudication decision to grant or deny a USCIS benefit. Failure to submit such information may prohibit USCIS from processing and properly adjudicating the benefit request and thus precludes the benefit requestor from receiving the benefit.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that the public may not be aware that ICE and CBP have access to USCIS ELIS data.

Mitigation: This risk is mitigated. USCIS provides general notice to individuals through the publication of this PIA that ICE and CBP may access USCIS ELIS data. USCIS also provides notice through its Privacy Notices that USCIS may share this information, as appropriate, for law enforcement purposes or in the interest of national security.



Privacy Risk: There is a risk that the public may not be aware that their information is stored in USCIS ELIS because the user only interacts with the MyUSCIS Account Experience.

Mitigation: This risk is partially mitigated. USCIS issued this PIA and the DHS/USCIS/PIA-071 MyUSCIS Account Experience⁵⁸ to serve as notice that MyUSCIS Account Experience replaces all aspects of the public-facing USCIS ELIS, and that USCIS ELIS continues to serve as an internal electronic case management system for certain benefit request forms.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

USCIS ELIS serves as the electronic record of an individual's immigration history. The system is also used to facilitate and track the adjudication of certain benefit requests. USCIS has many retention schedules to cover different types of data in USCIS ELIS, including the A-File, draft and filed forms, and systems.

Electronic Records

An individual's immigration history may be contained in the following materials and formats: (1) A paper A-File; (2) an electronic record in EDMS or USCIS ELIS; or (3) a combination of paper and electronic records and supporting documentation. USCIS ELIS maintains certain benefit request forms filed with USCIS. All documentation submitted or created in support of a USCIS benefit request is maintained in accordance with USCIS policy and NARA retention schedules after being scanned into USCIS ELIS. Benefit request forms that were rejected because the form was incomplete and/or not accompanied by the required signature or fee are maintained for 6 years or less.⁵⁹ These records have temporary value because they have little or no research value. All other benefit request forms and other electronic records in USCIS ELIS are designated as A-File records. A-File records are permanent, whether hard copy or electronic. These records have permanent value because they document enduring legal rights and have high potential research value. DHS transfers A-Files to the custody of NARA for retention for 100 years after the individual's date of birth.

USCIS ELIS Case Management

ELIS also serves as the electronic case processing, adjudication, and management functions of certain filed benefit request forms with USCIS. The case management data in USCIS ELIS is covered by the retention schedule for each form type. USCIS will update Appendix A to this PIA for each form retention schedule.

⁵⁸ See DHS/USCIS/PIA-071 MyUSCIS Account Experience, available at www.dhs.gov/privacy.

⁵⁹ Please see Appendix A to view the USCIS Approved NARA Schedule for Form Types.



5.2 Privacy Impact Analysis: Related to Retention

There is no risk associated with retention for USCIS ELIS. USCIS has a NARA-approved retention schedule for the electronic record and case management components of USCIS ELIS.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

USCIS shares information from USCIS ELIS with external federal agencies for the purpose of processing applications or petitions for benefits under the INA. USCIS may also share information with federal, state, local, and foreign government agencies and authorized organizations in accordance with approved routine uses, as described in the associated published system of records notices.

Department of State (DOS)

USCIS and DOS are partners in the processing of immigration benefit cases.⁶⁰ DOS has read-only access to USCIS ELIS data through PCQS. Access to USCIS ELIS provides DOS consular officers with information on USCIS adjudications of benefits and other decisions relating to non-immigrant and immigrant visas and naturalization cases. This includes data on pending benefit request forms, as well as historical information. This data sharing arrangement allows USCIS and DHS to increase processing efficiency and maintain a comprehensive picture of a benefit requestors' status from visa application to naturalization. It will reduce the likelihood that an individual or group might obtain an immigration benefit under the INA through fraud or error.

USCIS ELIS queries the DOS Consolidated Consular Database (CCD) to retrieve Immigrant Visa data, which includes biographic data, case data, photo, and fingerprint identification number (FIN).⁶¹ Immigrant Visa issuance data from the DOS is sent in a daily batch and ingested into USCIS ELIS. The data includes biographic data, visa case data, visa identification number, visa issuance date, class of admission, date of entry, and port of entry.

Social Security Administration (SSA)

USCIS, DOS, and the SSA currently have a Memorandum of Understanding (MOU) in place that covers the process by which SSA works with USCIS to issue SSNs and Social Security

⁶⁰ Memorandum of Agreement between the Department of State and the Department of Homeland Security regarding the sharing of visa and passport records and immigration and naturalization and citizenship records, signed November 18, 2008.

⁶¹ See DOS CCD PIA (July 17, 2015), available at <https://www.state.gov/documents/organization/242316.pdf>.



Homeland Security

Privacy Impact Assessment
DHS/USCIS/PIA-056(a) USCIS ELIS
Page 26

cards for immigrants through a process called Enumeration at Entry (EAE).⁶² As part of the DOS immigrant visa application process, immigrants outside the United States have the option to apply for an SSN card at the same time they apply for an immigrant visa. Once DOS approves their visa application and DHS admits them into the United States for permanent residence, SSA automatically issues the SSN card. USCIS ELIS electronically transmits to SSA enumeration data for resident aliens with employment authorization who request a SSN or replacement Social Security card. This process will allow USCIS benefit seekers to request a SSN or replacement card as part of the USCIS benefit process. USCIS ELIS sends requests for SSN issuance for approved Employment Authorization Documents cases when the requestor checks the appropriate boxes when filing the I-765.⁶³

Department of Justice (DOJ) Executive Office of Immigration Reform (EOIR)

USCIS ELIS queries Case Access System for EOIR⁶⁴ (CASE) for information related to the requestor to see if there has been any activity related to USCIS ELIS cases where a decision has been challenged by the applicant and/or the attorney/representative.⁶⁵ Where there is a case, USCIS looks at data such as case type, data case was filed with EOIR, case filing, case decision, case disposition, and document type.

U.S. Postal Service (USPS)

USCIS ELIS sends the address provided by the benefit seeker and receives USPS standardized addresses from the USPS Address Standardization Web Tool called Address Matching for Mail Processing. The USPS Address Standardization Web Tool corrects errors in street addresses, including abbreviations and missing information, and supplies ZIP Codes and ZIP Codes + 4. It supports up to five lookups per transaction.⁶⁶

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Department of State (DOS)

Sharing USCIS ELIS data via PCQS to DOS is compatible with the purpose of the system because the DOS mission, like that of USCIS, includes ensuring lawful visits and immigration to the United States as dictated by the INA. This sharing is covered by the Routine Use “I” of the

⁶² Memorandum of Understanding between Social Security Administration and Immigration and Naturalization Service (MOU), dated December 18, 2000. The party noted as the Immigration and Naturalization Service is now known as U.S. Citizenship and Immigration Services (USCIS). Provisions included in and addressed by the MOU are still applicable today.

⁶³ Form I-765 includes checkboxes that allow USCIS to share information with SSA for employment benefits.

⁶⁴ <https://www.justice.gov/EOIR/major-information-systems>.

⁶⁵ See DOJ EOIR-001 Records and Management Information System, 82 FR 24147, May 25, 2017.

⁶⁶ See USPS Address Matching for Mail Processing at

https://about.usps.com/handbooks/as353/as353apdx_042.htm#ep1181417.



Homeland Security

Privacy Impact Assessment DHS/USCIS/PIA-056(a) USCIS ELIS Page 27

DHS/USCIS-007 SORN,⁶⁷ which states that data may be shared with “Department of State for the purpose of assisting in the processing of benefit requests under the Immigration and Nationality Act, and all other immigration and nationality laws including treaties and reciprocal agreements.”

SSA

Sharing USCIS data with SSA is compatible with the purpose of the system because Section 205(b)(2) of the Social Security Act, as amended, authorizes SSA to issue a Social Security card to aliens at the time of their lawful admission to the United States. Routine Use “S” of the DHS/USCIS-007 SORN permits USCIS to share information with the SSA for the purpose of issuing a Social Security number and card to an alien who has made a request for a Social Security number as part of the immigration process in accordance with any related agreements in effect between the SSA, the DHS, and the Department of Labor entered into pursuant to 20 CFR 422.103(b)(3), 422.103(c), and 422.106(a), or other relevant laws and regulations.

Department of Justice (DOJ)

Sharing USCIS ELIS data with DOJ EOIR is compatible with the purpose of the system because the EOIR mission is to administer the immigration court system. The sharing of information is covered by the Routine Use “A” of the DHS/USCIS-007 SORN, which states that data may be shared with “DOJ, including Offices of the United States Attorneys, or other federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a part of the litigation or has an interest in such litigation.”

USPS

USCIS shares a limited amount of information with USPS for the purpose of enabling USPS and USCIS mission requirements. USCIS is required to collect fees, adjudicate benefit request forms, and provide timely evidence of the approved benefit. As part of normal operating procedures, USCIS contracts with USPS to serve as a courier service to transport and deliver documents to the recipient.

6.3 Does the project place limitations on re-dissemination?

Yes. DHS or USCIS enters into Memoranda of Understanding/Agreement (MOU/A) with external organizations prior to the systematic sharing of information. When sharing information with parties outside of DHS, the same specifications related to security and safeguarding of privacy-sensitive information that are in place for USCIS and DHS are applied to the outside entity. The agreements between DHS and external entities (e.g., DOS and SSA) fully outline responsibilities of the parties, security standards, and limits of use of the information, including

⁶⁷ 81 FR 72069 (Oct. 19, 2016).



re-dissemination, prior to information sharing. Access to records is governed by need-to-know criteria that demand the receiving entity demonstrate the mission-related need for the data before access is granted. In the terms of a negotiated agreement or the language of an authorization providing information to an external agency, USCIS includes justification for collecting the data, and an acknowledgement that the receiving agency will not share the information without USCIS or DHS's permission, as applicable.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

USCIS keeps an electronic record of all USCIS ELIS records sent to non-DHS partners. Furthermore, USCIS updates individual USCIS ELIS case records to reflect that a specific check (i.e., background or security check) has been completed.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that data shared by USCIS with external partners will be used beyond the original purpose of collection (immigration benefits).

Mitigation: USCIS is careful to share data with external agencies that have a need to know and put the information to a use that is compatible with USCIS SORNs. USCIS documents these safeguards in MOU/MOA with the external partners to ensure information shared is not used beyond the original purpose of collection (immigration benefits). All prospective information handlers must be authorized and complete privacy and security training before gaining access to the information. This mitigates the risk of unauthorized disclosure by requiring a trained employee with access to the information to review the information before sharing with an external agency.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

USCIS provide individuals with multiple avenues to access their information. Individuals who hold online accounts may access their case information maintained in USCIS ELIS through the MyUSCIS Account Experience. MyUSCIS Account Experience allows account holders to directly and securely engage with USCIS to obtain case-related information. Account holders who create online accounts must authenticate their access using their credentials and authentication code. Once authenticated, individuals may access their accounts including the information they used to create their profiles, such as name and address information. The information individuals may access includes a copy of the application they submitted, any notices or notifications generated by USCIS, and information about the status of their application.



An individual seeking access to more of his or her information held by USCIS may gain access to his or her records by filing a Freedom of Information Act (FOIA) or Privacy Act request. Individuals not covered by the Privacy Act or Judicial Redress Act (JRA) still may obtain access to records consistent with FOIA unless disclosure is prohibited by law or if the agency reasonably foresees that disclosure would harm an interest protected by an exemption. Any individual seeking access to his or her information should direct his or her request to the following address:

National Records Center
 Freedom of Information Act/Privacy Act Program
 P. O. Box 648010
 Lee's Summit, MO 64064-8010

Certain information requested may be exempt from disclosure under the Privacy Act because records related to fraud, with respect to an individual, may sometimes contain law enforcement sensitive information. The release of law enforcement sensitive information could possibly compromise ongoing criminal investigations. Further information for Privacy Act and FOIA requests for USCIS records can also be found at <http://www.uscis.gov>.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

USCIS allows individuals with an online account to correct any information in their benefit request form up until they electronically sign and submit the benefit request form through MyUSCIS Account Experience. After the benefit request has been submitted, the only changes the benefit requestor or legal representative may make are at the account level, such as updating an email address or other contact information. If the benefit requestor or legal representative need to correct inaccurate information on the benefit request form while the benefit is being adjudicated, he or she may submit the request in writing and upload the request into MyUSCIS Account Experience as unsolicited evidence or by mail. It is the adjudicator's decision to incorporate the corrected information, depending on the timing and validity of the information. For corrections after the application has been adjudicated, the requestor would use the existing FOIA and Privacy Act processes employed by USCIS, which depend on the type and context of the correction requested.

Additionally, U.S. citizens and lawful permanent residents, as well as other persons with records covered by the JRA, are afforded the ability to correct information by filing a Privacy Act Amendment request under the Privacy Act. Covered individuals should submit requests to contest or amend information contained in USCIS ELIS as discussed in Section 7.1. Individuals may direct all requests to contest or amend information to the USCIS FOIA/PA Office. Requests must state clearly and concisely the information being contested, the reason for contesting it, the proposed amendment, and clearly mark the envelope "Privacy Act Amendment." This would only apply to



Homeland Security

amendment of USCIS-held information. Persons not covered by the Privacy Act or JRA are not able to amend their records through FOIA. Should a non-U.S. person find inaccurate information in his or her record received through FOIA, he or she may visit a local USCIS Field Office to identify and amend inaccurate records with evidence.

7.3 How does the project notify individuals about the procedures for correcting their information?

Individuals are notified about procedures for correcting their information through MyUSCIS online account, Privacy Notices, the USCIS website, the NCSC, this PIA, and relevant SORNs.

7.4 Privacy Impact Analysis: Related to Redress

There is no privacy risk with respect to redress. Throughout the benefit request process, USCIS provides requestors multiple avenues to correct information. There is a process to update records during the adjudication process and to respond to information received from other sources. The information requested may be exempt from disclosure under the Privacy Act because information contained within USCIS ELIS may contain law enforcement sensitive information, the release of which could possibly compromise ongoing criminal investigations.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

USCIS ensures that practices stated in this PIA comply with internal federal, DHS, and USCIS policies. This includes the USCIS privacy policies, SOPs, information sharing agreements, orientation and training, rules of behavior, and auditing and accountability. USCIS ELIS is built off of the Amazon Web Services (AWS) US East/West cloud platform. AWS is a multi-tenant public cloud designed to meet a wide range of security and privacy requirements (e.g., administrative, operational, and technical controls) that is used by USCIS to protect data in accordance with federal security guidelines.⁶⁸ AWS is FedRAMP-approved and is authorized to host PII.⁶⁹ FedRAMP is a U.S. government-wide program that delivers a standard approach to the security assessment, authorization and continuous monitoring for cloud services.

USCIS employs technical and security controls to preserve the confidentiality, integrity, and availability of the data, which are validated during the security authorization process and on

⁶⁸ Public clouds are owned and operated by third-party service providers whereas private clouds are those that are built exclusively for an individual enterprise.

⁶⁹ <https://marketplace.fedramp.gov/#/product/aws-us-eastwest?status=Compliant&sort=productName>.



an ongoing basis. These controls mitigate privacy risks associated with authorized and unauthorized uses, namely misuse and inappropriate dissemination of data. USCIS ELIS has sophisticated role-based user access for operational users, as well as read-only users. These include roles that separate duties for operators to ensure appropriate oversight of the adjudication, as well as two levels of read-only roles to protect more sensitive data about a requestor from being accessible to internal users who only have a need for some of the data. Additionally, USCIS ELIS captures all user activity, including information changed and viewed, in audit logs, which are logged, tracked, and reviewed on a weekly basis as required by the USCIS Ongoing Authorization program.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

USCIS employees and contractors are required to complete annual Privacy and Computer Security Awareness Training to ensure their understanding of proper handling and securing of PII. The Privacy Awareness training addresses appropriate privacy concerns, including Privacy Act obligations (e.g., SORNs, Privacy Act Statements). The Computer Security Awareness training examines appropriate technical, physical, personnel, and administrative controls to safeguard information. USCIS provides USCIS ELIS users system-specific training on proper handling of PII, as well as appropriate use of data according to each role.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

USCIS deploys user role-based access controls and enforces a separation of duties to limit access to only those individuals who have a need-to-know in order to perform their duties. Each operational role is mapped to the set of system authorizations required to support the intended duties of the role. The mapping of roles to associated authorizations enhances adherence to the principle of least privilege. Authorized users are broken into specific classes with appropriate access rights. This need-to-know is determined by the respective responsibilities of the employee. These are enforced through DHS and USCIS access request forms and procedures. Access permissions are periodically reviewed to ensure users are only given access to the system based on a need-to-know.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

USCIS has a formal review and approval process in place for new sharing agreements. USCIS ELIS data is subject to the USCIS formal review process for any data sharing agreements.



Homeland Security

Privacy Impact Assessment DHS/USCIS/PIA-056(a) USCIS ELIS Page 32

That process includes, at a minimum, review by the Privacy Office, Counsel, and program officials entrusted with security of the data.

8.5 **Privacy Impact Analysis: Related to the Accountability and Integrity of the Information.**

Privacy Risk: The data maintained by Amazon Web Services (AWS) for the purposes of cloud hosting may be vulnerable to breach because security controls may not meet system security levels required by DHS.

Mitigation: This risk is mitigated. USCIS is responsible for all PII associated with the ELIS system, whether on a USCIS infrastructure or on a vendor's infrastructure, and it therefore imposes strict requirements on vendors for safeguarding PII data. This includes adherence to the DHS 4300A Sensitive Systems Handbook, which provides implementation criteria for the rigorous requirements mandated by DHS's Information Security Program.⁷⁰

Responsible Officials

Donald K. Hawkins
 Privacy Officer
 U.S. Citizenship and Immigration Services
 Department of Homeland Security

Approval Signature

[Signed copy complete and on file with the DHS Privacy Office]

Philip S. Kaplan
 Chief Privacy Officer
 Department of Homeland Security

⁷⁰ See <https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook>.



Homeland Security

Appendix A
 USCIS Approved NARA Schedule for Form Types

<u>Form Number</u>	<u>Form Name</u>	<u>NARA Approved Schedule</u>
I-90	Application to Replace Permanent Resident Card	DAA-0566-2015-0004
I-131	Application For Travel Document	DAA-0566-2016-0004
I-765	Application for Employment Authorization	DAA-0566-2016-0005
I-821	Application for Temporary Protected Status	DAA-0566-2016-0007
Form I-821-D	Consideration of Deferred Action for Childhood Arrivals	DAA-0566-2016-0006
N-400	Application for Naturalization	DAA-0566-2016-0002


Appendix B
USCIS Benefit and Service Types Processed in USCIS ELIS

Form Number	Form Name	Paper Filings	Online Filings
DOS Immigrant Visa Packet (includes data from DS-260 and I-864)	DOS Immigrant Visa Packet		X
G-28	Notice of Entry of Appearance as Attorney or Accredited Representative [OMB No. 1615-0105]	X	X
I-90	Replacement of Permanent Resident Card [OMB No. 1615-0082]	X	X
I-130	Petition for Alien Relative [OMB No. 1615-0012]	X	X
I-131	Application for Travel Document [OMB No. 1615-0013]	X	
I-131A	Application for Travel Document (Carrier Documentation) [OMB No. 1615-0135]	X	
I-212	Application for Permission to Reapply for Admission into the United States After Deportation or Removal [OMB No. 1615-0018]	X	
I-356	Request for Cancellation of Public Charge Bond [OMB No. 1615-0141]	X	
I-590	Registration for Classification as Refugee [OMB No. 1615-0068]	X	X
I-765	Application for Employment Authorization [OMB No. 1615-0040]	X	X
I-765WS	Application for Employment Authorization Worksheet [OMB No. 1615-0040]	X	



Homeland Security

Privacy Impact Assessment
 DHS/USCIS/PIA-056(a) USCIS ELIS
 Page 35

I-821	Application for Temporary Protected Status [OMB No. 1615-0043]	X	X
I-821D	Consideration of Deferred Action for Childhood Arrivals [OMB No. 1615-0124]	X	X
I-912	Request for Fee Waiver [OMB No. 1615-0116]	X	
I-944	Declaration of Self-Sufficiency [OMB No. 1615-0142]	X	
I-945	Public Charge Bond [OMB No. 1615-0143]	X	
N-400	Application for Naturalization [OMB No. 1615-0052]	X	X
N-336	Request for a Hearing on a Decision in Naturalization Proceedings Under Section 336 [OMB No. 1615-0050]	X	X
N-565	Application for Replacement Naturalization/Citizenship Document [OMB No. 1615-0091]	X	X
N-600	Application for Certificate of Citizenship [OMB No. 1615-0057]	X	X
N-600K	Application for Citizenship and Issuance of Certificate Under Section 322 [OMB No. 1615-0087]	X	X



Privacy Impact Assessment
for the
myUSCIS Account Experience

DHS/USCIS/PIA-071

December 15, 2017

Contact Point
Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
(202) 272-8030

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1664



Abstract

U.S. Citizenship and Immigration Services (USCIS) operates myUSCIS Account Experience to engage benefit requestors and legal representatives, while they navigate and complete the immigration process, through an authenticated digital account experience. MyUSCIS Account Experience offers a personalized, authenticated, and secured account for benefit requestors and legal representatives, and replaces all aspects of the public facing USCIS Electronic Immigration System (USCIS ELIS).¹ This Privacy Impact Assessment (PIA) evaluates the privacy risks and mitigations associated with the collection, use, and maintenance of personally identifiable information (PII). USCIS plans to update the appendices of the PIA as subsequent services and functionalities are added to myUSCIS Account Experience.

Overview

U.S. Citizenship and Immigration Services (USCIS) is the component of the Department of Homeland Security (DHS) that oversees lawful immigration to the United States. This mission includes receiving and adjudicating a wide variety of immigration and non-immigration benefits and requests (hereafter referred to as *immigration benefits*). USCIS historically operated under a paper form intake process requiring USCIS adjudicators to use a variety of case management systems to adjudicate the benefit request and issue written notices. During this time, USCIS only offered live assistance for individuals seeking case assistance or updates through the National Customer Service Center (NCSC) and field office visits.² Further, benefit requestors experienced an unauthenticated and fragmented online experience, or extended wait-times from NCSC and the local field office, and could only access limited information about pending benefit filings.

As part of its mission, USCIS is striving to expand opportunities for individuals to further engage with USCIS. USCIS is endeavoring to provide individuals reliable and up-to-date access to general and pending case information. USCIS established the myUSCIS Account Experience to offer customers an authenticated and holistic online experience. The purpose of myUSCIS Account Experience is to integrate personalized digital services for a seamless end-to-end online experience through a secure USCIS online account. Through myUSCIS Account Experience, individuals are able to create a personal account to securely use digital services that supports the benefit request process and allows access to pending case information. MyUSCIS Account Experience will replace all aspects of the public-facing USCIS Electronic Immigration System

¹ See DHS/USCIS/PIA-056 USCIS Electronic Immigration System (USCIS ELIS), available at www.dhs.gov/privacy.

² See DHS/USCIS-PIA-054 National Customer Service Center, available at www.dhs.gov/privacy.



Homeland Security

Privacy Impact Assessment

DHS/USCIS/PIA-071

myUSCIS Account Experience

Page 2

(USCIS ELIS).³ USCIS ELIS continues to serve as an internal electronic case management system that allows USCIS adjudicators to process certain benefit request forms.

myUSCIS Account Experience offers the following six core digital modules along with several supporting functions and capabilities:

1. **Onboarding** allows account holders to establish a secure account with USCIS.
2. **Account Home** serves as the central location for account holders to manage their case with USCIS.
3. **Digital Forms** allows individuals to electronically file applications and petitions.
4. **Case Activity** offers a holistic view of a single case as well as a view into a customer's full immigration history with USCIS.
5. **Document Center** serves as a repository of documents and notices specific to the account holder that are integral to the immigration process.
6. **Secure Messaging** provides access to live assistance within the account.

This secure online account allows individuals to manage their account, profile, and case information with USCIS. Together, these modules provide individuals with a cohesive experience.

myUSCIS Account Experience is an expanding initiative with several supporting services to contribute to the overall immigration experience of individuals. As myUSCIS Account Experience includes additional support services, USCIS plans to update the Appendix to this PIA to evaluate risks and mitigation strategies of each support service.

This PIA examines each module further to discuss the personally identifiable information (PII) USCIS collects, uses, and maintains while using myUSCIS Account Experience.

Account Creation

myUSCIS Account Experience allows benefit requestors and legal representatives to create a USCIS online account through <https://myaccount.uscis.dhs.gov/>. To create an account, an individual enters an email address into an online form. USCIS sends a confirmation email to the provided address for accuracy. The email address is then stored as the account holder's username. The account holder creates a strong password, and provides answers to security questions that he or she will be asked to reset the account password in the future. The security questions are "fill-in-the-blank" questions the customer provides the answer during account set-up. USCIS provides the customer with a dropdown menu of standard questions, and the customer chooses which ones to use as his or her security questions. USCIS will not use the answers to these questions for

³ See DHS/USCIS/PIA-056 USCIS Electronic Immigration System (USCIS ELIS), available at www.dhs.gov/privacy.



Homeland Security

Privacy Impact Assessment

DHS/USCIS/PIA-071

myUSCIS Account Experience

Page 3

purposes other than assisting with password resets (e.g., the answers would not be available to adjudicators for an immigration benefit purpose or fraud investigators in the event of a fraud investigation).

myUSCIS Account Experience passwords and answers to the security questions are centrally stored within the USCIS Identity, Credential and Access Management (ICAM) system. Passwords are not visible. The answers to the security questions are only visible to USCIS customer helpdesk personnel who assist account holders in resetting their passwords. USCIS ICAM provides myUSCIS with account credentialing, account authentication, and identity verification for account holders. ICAM collects this initial information. The USCIS online account includes account information, profile information, and availability for online filing.

Two Factor Authentication

To complete the onboarding process, USCIS sets a two-factor authentication code preference for integrity and authenticity assurance purposes. Each time the individual logs-in, myUSCIS forwards an authentication code through an email or SMS, or through the use of a third-party authenticator application as part of his or her logon credentials. If the account holder chooses to use a third party authentication application, he or she is provided instructions on how to connect to the authentication application. The selection and use of a third-party application is at the discretion of the account holder. The account holder can use any authentication application available on the smart device of his or her choice. USCIS does not prescribe a specific authenticator application. A separate USCIS notice informs the account holder to familiarize him or herself with the privacy policy of the third party application since USCIS has no control over the third party policies. The user credentials are sent to the USCIS ICAM system for verification and authentication.

Identity Proofing

USCIS provides remote identity proofing using Identity Proofing as a Service (IDPaaS). IDPaaS is a challenge-response system utilizing shared knowledge likely to be known to USCIS and the myUSCIS account holder but unlikely to be known to third parties. This challenge-response system draws questions based on information contained within the Central Index System (CIS),⁴ originally derived from other USCIS systems, DHS systems, including U.S. Customs and Border Protection (CBP), and Department of State (DOS) systems.

Potential questions may ask on what street an applicant lived or what DOS post his or her immigrant visa was granted. This is similar to how some commercial applications in the United States verify the identity of application account holders. Account holders who are required to use IDPaaS are provided a notice explaining what identity proofing is and what to expect before

⁴ See DHS/USCIS/PIA-009 Central Index System, available at www.dhs.gov/privacy, to learn more about CIS and view system USCIS, DHS, and DOS interfaces used develop challenge questions in support of identity proofing.



Homeland Security

Privacy Impact Assessment

DHS/USCIS/PIA-071

myUSCIS Account Experience

Page 4

launching into the process. If account holders are unable to pass the IDPaaS questionnaire, they are presented with instructions on how to proceed on an alternate identity proofing path, which may be contacting NCSC or appearing in-person at a USCIS field office. Once the account holder passes the identity proofing quiz, myUSCIS Account Experience retains the fact that the account holder has been identity-proofed and does not require the account holder to repeat the process for subsequent immigration benefit requests.

The questions presented to each account holder are dynamically generated based on the best information USCIS has about the account holder in CIS and the most diverse set of questions available. This data originally comes from information the DOS collected in-person when issuing a visa, information CBP collected in-person upon entry at the border, and information USCIS has collected from the account holder based on previous immigration benefit requests. In designing the questionnaire, USCIS looks at the breadth of data and categorizes it into several domains based upon the type of information, such as travel, contact information, etc. The questionnaire is designed to ask the account holder questions from different domains to ensure the account holder is showing knowledge of a wide breadth of data about him or herself and also data that would not be known by a different person. IDPaaS may allow account holders more than one attempt to pass the questionnaire, but only if the system has enough reliable data in enough domains about the account holder. Questions are in multiple-choice format and include a “none of the above” option, when appropriate.

Account Home

The myUSCIS Account Experience homepage serves as the central location for account holders. Account holders are able to save information throughout the benefit filing process and return at a later time to submit or delete their draft case. Account holders who successfully submit their case are able to manage their active cases from the beginning until the end. From the dashboard, account holders are able to:

- Select notifications options. As part of the account experience, the account holder can receive notifications when there is a change in status. These alerts are sent via email or text depending on the preference set by the account holder at the time of account creation. These text or email alerts only provide notice that there has been a change to the case. The account holder has the option to log in to the myUSCIS online account for additional information;
- Manage draft e-file forms;
- Access documents and notices;
- Start and send a secured message to USCIS;
- Request an update to his or her profile;



- View current status of any case and immediate next steps; and
- View estimated processing time for a benefit request and next milestone in case lifecycle.

Digital Forms

USCIS allows certain benefit request forms and service types to be completed and filed by benefit requestors and/or legal representatives through their myUSCIS account.

The Digital Form module is an interactive tool that assists individuals with completing immigration benefit request forms or service types. The digital benefit request forms collect the same information as the corresponding paper form. Prior to initiating the request, USCIS provides the account holder with a Privacy Notice covering the particular benefit request at the time of that collection. The immigration benefit request forms and service types are dynamic meaning that questions dynamically expand or become disabled as the account holder progresses through the request. In other words, an account holder's answer to one question may prevent a series of additional questions from being necessary. This enables the customer to respond only to applicable questions. The account holder may edit, delete, or update information when the form is in draft state. The system does not keep copies of these previous iterations. Prior to the submission of the benefit request form, the account holder has the opportunity to review the information entered as part of benefit request form or service type. A draft case is deleted if inactive for 30 days.

Account holders who are assisted by a legal representative on a specific immigration case must complete Form G-28, *Notice of Entry of Appearance as Attorney or Accredited Representative*, and file it with USCIS. This can be accomplished online via myUSCIS Account Experience or on paper via the USCIS Lockbox service.⁵ If a paper filing for an immigration benefit type is submitted with a Form G-28, the Lockbox transmits the information to USCIS ELIS. myUSCIS Account Experience interfaces with USCIS ELIS and conducts a search to identify whether the legal representative already has a USCIS representative account in the system. If a legal representative account already exists, the new filing is linked to the existing account. If a legal representative account does not exist, the legal representative can create a USCIS online account through the myUSCIS Account Experience.

⁵ Lockbox facilities are operated by a specialized contractor authorized by the Department of Treasury (Treasury). This contractor manages the intake of USCIS benefit applications and the collection of associated fees submitted directly by mail. It provides the mechanisms to capture information electronically from USCIS benefit request forms, deposit associated fees, move the information to USCIS systems via a system interface, and generate acceptance and rejection notices to applicants. The contractor is also responsible for preparing the application-related files in accordance with USCIS guidance and sending the files to the next processing site (i.e., Service Center). The contractor does not approve or deny benefit request forms received by the USCIS Lockbox. See Department of Treasury Financial Management Service Privacy Impact Assessment, available at https://www.fms.treas.gov/pia/ECP_PIA.pdf.



Homeland Security

Privacy Impact Assessment

DHS/USCIS/PIA-071

myUSCIS Account Experience

Page 6

Legal representatives may also electronically file requests in myUSCIS Account Experience. To successfully submit a filing in myUSCIS, both the legal representative and his or her client (i.e., the USCIS benefit requestor) must have their own, independent USCIS online account. The legal representative uses his or her account to draft a request on behalf of the benefit requestor. Upon completion, the legal representative submits it to the benefit requestor for review. When the legal representative submits the draft benefit request for benefit requestor review, the legal representative provides myUSCIS Account Experience with the benefit requestor's email address. MyUSCIS Account Experience then presents the legal representative with a passcode that should be provided to the benefit requestor. The benefit requestor must provide the passcode in order to access the draft request.

myUSCIS Account Experience then sends the benefit requestor an email informing him or her about the pending draft in their existing account. When the benefit requestor logs into the system he or she is prompted to input the passcode in order to view the draft immigration request completed by the legal representative. myUSCIS Account Experience only gives the benefit requestor access to review the draft case if the email and passcode match. Upon review, the benefit requestor is able to reject the draft and send it back to the legal representative. The legal representative may then overwrite the previous draft and resubmit to the benefit requestor for review. However, a new passcode is required in order to access the revised document.

Once an account holder completes a benefit request and uploads necessary evidence, myUSCIS Account Experience requires the account holder to electronically sign the request and pay the applicable fee. Payment is made using the U.S. Department of Treasury's Pay.Gov service.⁶ USCIS does not collect the fee directly. Rather, the account holder is redirected to the Pay.Gov interface, and Pay.Gov collects payment information (e.g., credit card, debit card, or Automated Clearing House (ACH debit)) from a personal bank account and billing information. Once Pay.Gov validates the payment information, the account holder is routed back to myUSCIS Account Experience and the myUSCIS Account Experience confirms to the account holder that he or she successfully submitted the request.

Once the immigration request is submitted and accepted to USCIS, both the legal representative and the benefit requestor have access to the same processing requests and notices, as well as case status updates.⁷ If applicable, USCIS mails a receipt notice to the account holder's

⁶ See U.S. Department of Treasury Financial Management Services Pay.Gov Privacy Impact Assessment 2.0 (July 1, 2011), available at http://fms.treas.gov/pia/paygov_pia%20.pdf.

⁷ At any point during the benefit adjudication process, account holders may change their legal representative or elect to forgo legal representation during the adjudication of a benefit request. Notification to USCIS of the substitution or withdrawal of a legal representative may occur in a written notice of withdrawal by the representative of record or upon the filing of a properly completed G-28 by the new representative, include the receipt number associated with the substitution. USCIS updates the appropriate systems to remove and add access for the legal representative. The updated legal representative is then provided case access and issued correspondence related to the benefit request.



Homeland Security

Privacy Impact Assessment

DHS/USCIS/PIA-071

myUSCIS Account Experience

Page 7

physical address, as well as makes it available electronically through the myUSCIS Account Experience online account.

Case Activity

Case Activity provides current and past status updates and case processing times to account holders on pending immigration benefit requests filed through myUSCIS Account Experience. The case activity for electronically filed forms (for myUSCIS Account Experience only) is automatically updated based on the associated receipt number. The Case Activity modules notify the account holder of major milestones such as receipt of a benefit request form or upcoming biometric and interview appointments. The Case Activity module receives case status updates from Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR).⁸ Case updates associated with a receipt number are sent electronically on a daily basis to myUSCIS Account Experience. The Case Activity module provides the account holder with a detailed explanation of the case status. Account holders are able to use Case Status Online⁹ to obtain case updates for all forms filed outside of myUSCIS Account Experience.

Document Center

The Document Center serves as the document and notice repository for the account holder. In the Document Center, the account holder is able to upload and view evidence submitted in support of an electronically-filed or paper-filed application or petition, view notices issued by USCIS, and reuse evidence submitted previously for new forms or USCIS requests, in addition to searching, tagging, and sorting evidence and notices.

Case Evidence

USCIS requires initial evidence of proof of identification and justification of eligibility for a benefit or service by way of supporting documentation. Examples of supporting documentation include copies of birth, marriage, or adoption certificates; divorce decrees; affidavits of financial support; and/or school records. myUSCIS prompts the account holder to upload certain evidence based on the answers provided by the account holder while completing an application or petition. Account holders upload evidence by scanning documents and attaching the scanned images to a draft case or when responding to requests for additional information from USCIS.¹⁰ Account holders can also upload evidence during the application process as part of a request for evidence or as applicable.

⁸ See DHS/USCIS/PIA-023(a) Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR), available at www.dhs.gov/privacy.

⁹ See DHS/USCIS/PIA-019(b) Customer Relationship Interface System (CRIS), available at www.dhs.gov/privacy.

¹⁰ A request for evidence is made when an application/petition is lacking required documentation/evidence (initial evidence) or the USCIS adjudicator needs more documentation/evidence (additional evidence) to determine an applicant's eligibility for the benefit sought.



Homeland Security

Privacy Impact Assessment

DHS/USCIS/PIA-071

myUSCIS Account Experience

Page 8

USCIS Correspondence

Notices are written communications indicating that USCIS has taken an action regarding a request that may or may not require action by the benefit requestor. In accordance with the Immigration and Naturalization Act (INA), USCIS has a statutory obligation to provide the benefit requestor with notice of action USCIS takes related to a request, as well as provide information related to the status of a request. A notice has a legal effect with respect to the adjudication of the requested benefit, and conveys information that the individual has a right to know and USCIS has a legal duty to communicate.

USCIS issues the following notices to communicate with customers or convey a status of an immigration benefit:

- Receipt of benefit requests forms and payments;
- Rejection of benefit requests forms;
- Transfer of files;
- Re-open cases; and
- Appointments (i.e., fingerprint, biometric capture, interview, rescheduled).

USCIS sends notices to inform benefit requestors of any actions that the requestors may need to take or actions that have been taken by USCIS.

USCIS adjudicators issue Requests of Evidence (RFE) or Notices of Intent to Deny (NOID) when an application lacks required documentation or the adjudicator needs additional evidence to determine an applicant's eligibility for the benefit sought. These forms are also uploaded into the Document Center. Once officially submitted, USCIS adjudicators review the benefit request and supporting documents to ensure all information is present. In situations in which evidence is missing or all required initial evidence is submitted but does not establish eligibility, USCIS may request that the benefit requestor to supply additional information through an RFE or NOID for continued processing.

USCIS adjudicators use the Enterprise Correspondence Handling Online (ECHO) and Notice Generation Systems to generate notices while processing benefit requests for immigration benefits.¹¹ USCIS uploads notices from these systems to the myUSCIS Account Experience. All notices available in myUSCIS Account Experience are also printed and mailed to the benefit requestors and their legal representatives.

¹¹ See DHS/USCIS/PIA-063 Benefit Decision and Output Processes, available at www.dhs.gov/privacy.



Homeland Security

Privacy Impact Assessment

DHS/USCIS/PIA-071

myUSCIS Account Experience

Page 9

Secure Messaging

Secure messaging allows the account holder to send emails to USCIS while logged into his or her USCIS online account. To create a new email, the account holder clicks on the ‘new message’ button and a form is displayed. The authenticated form requests the subject, case receipt number, client name (legal representative only), and a text box to describe the issue.

The subject, case receipt number, and client name fields offer a drop down menu personalized for his or her account. When composing a secure message, the account holder is able to select one of the following options to autofill the subject line:

- A case already filed online;
- Filing an application online;
- Getting a confirmation or PIN via email;
- Getting an answer to a general question;
- Getting online filing to work in my browser;
- Making a payment; or
- Other (write subject in description).

The receipt number field is a drop down menu of active receipt numbers associated with that account holder’s pending applications. This reduces the risk of an account holder providing an incorrect number in this field. If the account holder is a legal representative, he or she must select the name of the client from a drop down menu as well.

An open textbox is available to the account holder to provide additional feedback. Since emails are associated with a specific profile, USCIS notifies account holders to exclude personal information, specifically Alien Number or Social Security number, in the subject or message. Each inquiry is assigned a system-generated service item number and all corresponding messages are tied to the service item number. When all fields are completed, the account holder may send the email. The encrypted message is routed to NCSC after the account holder hits send. USCIS researches each inquiry to assist the account holder with resolving the issue. Based on the outcome of his or her finding, USCIS creates a response letter to inform the account holder of how his or her inquiry was resolved. The account holder receives a text or email alert when USCIS responds to an inquiry. USCIS only discloses information related to the case. If additional identity verification is required, USCIS may contact the account holder with information on record. All the responses between USCIS and the account holder are stored in the Secure Message module.



Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The authority to collect information is found within the Immigration and Nationality Act (INA), 8 U.S.C. §§ 1103, 1201, and 1255.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The information collected, used, maintained, and stored in myUSCIS Account Experience is covered under the following SORNS:

- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records¹² covers documentation and maintenance of an individual's immigration application, petitions, and requests as he or she passes through the U.S. immigration process;
- DHS/USCIS-007 Benefits Information System¹³ permits USCIS' collection, use, maintenance, dissemination, and storage of paper and electronic benefit request information. This includes case processing and decisional data not included in the A-File SORN. It also covers case specific information that is collected and shared with online account holders; and
- DHS/ALL-037 E-Authentication Records System of Records¹⁴ covers information collected to create and authenticate an individual's identity for the purpose of obtaining a credential to electronically access a DHS program or application.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. myUSCIS was approved for operation on December 18, 2014, for a period of 36 months, unless a significant change to the information system required an earlier accreditation. The myUSCIS authority to operate (ATO) is set to expire on December 18, 2017. myUSCIS is undergoing the security authorization process and is to receive an update ATO upon completion of this PIA.

¹² DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (Oct. 18, 2017).

¹³ DHS/USCIS-007 Benefits Information System, 81 FR 72069 (Oct. 19, 2016).

¹⁴ DHS/ALL-037 E-Authentication Records System of Records, 79 FR 46857 (Aug. 11, 2014).



1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

No. USCIS is developing a retention schedule with NARA for myUSCIS that is subject to final approval. USCIS is proposing to maintain the masterfile data for 5 years and account registration data for 7.5 years.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The OMB Control number for online account creation is 1615-0122 (there is no corresponding agency number). Each benefit request form or service type filed through myUSCIS Account Experience has an existing OMB control number that covers the electronic information collection. An updated list is available in Appendix A and B.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

Account Creation

Benefit requestors and legal representatives are required to create separate accounts. To create an account, myUSCIS Account Experience collects name, physical address, home telephone number, mobile phone number, user name, user password, responses to security questions, and a USCIS-generated authentication code. For a legal representative profile, USCIS collects the organization name, bar number, licensing authority, accredited representation date, daytime phone number, fax number, mailing address, and an electronic signature to verify information.

Account Dashboard

The Account Dashboard serves as the central location for account holders to manage their case and relationship with USCIS. Account Dashboard serves as the access point of all the features of the online account.



Digital Forms and Services

The Digital Forms and Services module is an interactive tool that allows account holders to complete immigration benefit request forms or service requests electronically. The information collected from each benefit request form or service type varies and not all forms collect the same information. Generally, each form may collect the following information regarding benefit requestors and third party beneficiaries: full name, address, telephone number, date and place of birth, unique identifying numbers (i.e., Online Account Number, Alien Number, and SSN, citizenship/nationality, and gender. USCIS forms also collect information about the form preparer, interpreter, and legal representative. A full account of what data is requested for each immigration benefit and service type may be viewed by referencing the forms associated with each immigration benefit or service type in Appendix A and B.¹⁵

Case Activity

Case activity provides current and past status updates and case processing times to account holders on pending immigration benefit requests filed through myUSCIS Account Experience.¹⁶

Document Management

Document Management stores and maintains supplemental evidence uploaded from the account holder and notices uploaded from USCIS. Examples of supporting evidence include copies of civil documents such as birth, marriage, or adoption certificates; divorce decrees; affidavits of financial support; or school records. Examples of USCIS notices include receipt of benefit requests forms and payments, biometric appointments, RFEs, and NOIDs.

Secure Message

Secure Message allows account holders to email USCIS about a specific case inquiry. Each email contains fields that request the subject of the inquiry, associated case receipt number, and a text box to describe the issue. Legal representative email contains the same fields and also requests the client name. The subject, case receipt number, and client name (only in the legal representative account) include a drop down feature.

- **Subject:** The account holder is offered multiple short, descriptive reasons for the inquiry (e.g., a case already filed online, filing an application online, other (write subject in description) to select and populate the subject heading.
- **Case Information:** The benefit requestor is provided a list of receipt numbers for cases that were filed online and selects the receipt number associated with the inquiry. The

¹⁵ All USCIS Forms are available at <https://www.uscis.gov/forms>.

¹⁶ USCIS processes all case submissions in the order they are received. Processing times are an estimate based on the time it is currently taking to process the benefit request type submitted and the number of pending applications or petitions of the same type in the office where the account holder's case is pending.



legal representative account is provided with a list of client names and receipt numbers for cases that were filed online or associated to the representative with a G-28 on file and is able to select the appropriate case information relating to the inquiry.

- **Text box:** An open textbox is available for the account holder to provide additional feedback. Since emails are associated with a specific profile, USCIS notifies account holders to exclude personal information, specifically Alien Number or Social Security number, in the subject or message.

Each inquiry is assigned a system-generated service item number and all corresponding messages are tied to the service item number.

2.2 What are the sources of the information and how is the information collected for the project?

Information in myUSCIS Account Experience is derived from account holders (i.e., benefit requestors and accredited representatives) for account creation, benefit form and service types, secure messages, and supplemental evidence. USCIS systems and personnel to provide data for case activity, processing times, USCIS notices, and secure messages.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No.

2.4 Discuss how accuracy of the data is ensured.

myUSCIS Account Experience collects user profile, biographic information, and supplemental evidence directly from the account holder (i.e., individual or his or her representative); therefore, USCIS is dependent upon the accuracy of the information provided by the account holder. To ensure the accuracy and integrity of the information, account holders are provided with the opportunity to review and edit information prior to its submission.

myUSCIS also receives information from USCIS systems or personnel to share information. The myUSCIS Account Experience account is tied to a unique identifier that links the authentication services with myUSCIS and the USCIS systems. To ensure data accuracy, myUSCIS validates data through system coding to mitigate or prevent inconsistencies in account holder data (e.g., the system rejects 00/00/00 birthdates) and that only the account holder information is being shared to create the personalized experience.



2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that myUSCIS Account Experience collects more information than necessary to adjudicate a benefit request.

Mitigation: myUSCIS mitigates this risk in two main ways. First, the system only collects information pertaining to one case at a time, so that the account holder cannot be prompted to enter information unless it pertains to the specific case on which the account holder is working. Second, the user interface dynamically skips questions that are not relevant based on previous responses. For example, when a paper form would instruct the customer to skip a section of the form based on his or her answer, myUSCIS skips to relevant sections and questions. It is possible for account holders to upload more evidence than necessary because they are allowed to submit “unsolicited evidence” at any point until adjudication. This is a valuable feature that allows benefit requestors the opportunity to provide information initially forgotten or submitted incorrectly, which partially mitigates the risk that benefit requestors may opt to provide too much information.

Privacy Risk: myUSCIS Account Experience may capture outdated, inaccurate, irrelevant or incomplete information through the Digital Forms module.

Mitigation: This risk is mitigated because the account holder has the ability to review information prior to submission to USCIS. USCIS account holders provide information to myUSCIS Account Experience directly to ensure accuracy of information. Prior to the submission of information by the Digital Forms module, myUSCIS Account Experience provides the individual with an opportunity to enter biographic information, review its accuracy, and amend it. Information submitted by the legal representative requires the benefit requestor to review the filing prior to electronically signing the form. The benefit requestor is required to check a box attesting that he or she has reviewed the information. This ensures the accuracy and integrity of the benefit request form prior to submission.

Privacy Risk: There is a risk that inaccurate or outdated evidence is stored and maintained in the Document Center.

Mitigation: USCIS mitigates this risk by requiring the account holder to provide valid documentation as initial evidence. USCIS requires supporting documentation as initial evidence of a benefit requestor’s identification and eligibility for a benefit. Current and accurate documents are required for USCIS to make a decision on a benefit request. USCIS relies on the account holder to verify the veracity of the evidence. Account holders are responsible for ensuring the most up-to-date documents are uploaded and included as part of their benefit request. If the account holder identifies that the incorrect document was uploaded, the account holder is able to delete the incorrect document and upload a new document. Also, prior to electronically submitting the benefit



request to USCIS, myUSCIS Account Experience allows the account holder to review the information, as well the supporting evidence.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

myUSCIS Account Experience allows account holders to engage with USCIS in an authenticated account experience. Specific uses of myUSCIS Account Experience and the information it contains include:

- Create a user profile;
- Draft, manage, and file benefit request forms and service types. Cases are maintained in myUSCIS Account Experience until it is submitted and signed electronically. Once the filing has been submitted, the information is sent to USCIS ELIS or the appropriate case management system for adjudication;
- Maintain supplemental evidence submitted with an e-filed application and reuse evidence submitted previously for new forms or USCIS requests;
- View notices issued by USCIS;
- View estimated processing times for cases and next milestones in case lifecycles;
- View current status of a case and immediate next steps;
- Access documents and notices related to a particular status; and
- Initiate secure messages to USCIS and manage responses from USCIS.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

No. Access to the data stored in myUSCIS Account Experience, as well as the system, is limited to account holders.



3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that myUSCIS Account Experience will collect and use information in a manner inconsistent with USCIS' authority and mission.

Mitigation: USCIS mitigates the risk by minimizing the amount of information collected and by limiting the purposes for which USCIS may use the information. MyUSCIS Account Experience offers account holders with a secure online account to engage with USCIS. Access to the data stored in myUSCIS Account Experience, as well as the system, is limited to account holders. USCIS adjudicators do not have access the account holder information until it is officially submitted for USCIS review. USCIS systems administrator and help desk support have limited access to the account holder's account login information to assist with technical issues.

Privacy Risk: There is a risk that USCIS may access and use benefit information prior to the official submission of the benefit request.

Mitigation: USCIS mitigates this risk by restricting secure profile access to account holders (i.e., benefit requestors and legal representatives). While using myUSCIS Account Experience, account holders are able to save draft benefit request forms and upload supplemental evidence. The account holder may edit, delete, or update information when it is in draft state and the system does not keep copies of these previous iterations. This preserves the same confidentiality for an electronic filing as a paper filing. USCIS adjudicators do not have access to this information until the account holder submits the filing to USCIS, in which the information is routed to USCIS ELIS or other case management system. This risk is further mitigated by limiting the retention of draft forms in the system to 30 days from the date of last action on the form.

Privacy Risk: There is a risk that USCIS may access and use uploaded, not officially submitted, evidence maintained in the Document Center.

Mitigation: USCIS mitigates this risk by restricting access to information maintained in secure profile to the account holder only. USCIS adjudicators do not have access to documents stored in the Document Center or any other module of the secure profile. Account holders are limited to benefit requestors and legal representatives. The account holder must electronically submit the benefit request form and appended support evidence for USCIS to use the information for adjudication purposes. Once officially submitted, the benefit request is transferred to USCIS ELIS, or other case management system for review and adjudication. USCIS adjudicates the benefit request using only the information maintained in USCIS ELIS through normal processing procedures.

Privacy Risk: There is a risk that myUSCIS Account Experience will inadvertently disclose information about a different account holder.

Mitigation: USCIS mitigates this risk by implementing multiple security controls. First,



USCIS configured the interconnecting systems to link and share information associated with the same receipt number. Second, an account holder only has access to his or her own cases. This prevents information from being submitted for the incorrect individual. Lastly, legal representatives must select the receipt number and name of the client to upload the evidence. In addition, for final submission, the client (applicant) must validate the submission through his or her own account.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

USCIS provides general notice to account holders through the publication of this PIA, associated SORNs, and through the USCIS website. Additionally, myUSCIS Account Experience provides a Privacy Notice prior to the submission of any information. The Privacy Notice notifies the account holder about the authority to collect the information requested, the purposes of collection, USCIS' routine uses of the information, and the consequences of an account holder providing or declining to provide the information to USCIS.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

USCIS informs the account holder that providing information is voluntary. An account holder can choose to decline to provide information. However, this may prevent the account holder from using the myUSCIS Account Experience. By using myUSCIS Account Experience, the account holder is implying consent to USCIS' uses of information.

4.3 Privacy Impact Analysis: Related to Notice

There is no privacy risk related to notice. All information collected by myUSCIS is provided directly from the account holder. The account holder is provided a Privacy Notice prior to submitting any information to USCIS. Additionally, USCIS provides notice to individuals through this PIA, and associated SORNs.



Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

USCIS is developing a retention schedule for myUSCIS Account Experience that is subject to final approval by NARA. USCIS is proposing to maintain the masterfile data for 5 years and account registration data for 7.5 years.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: myUSCIS does not have a records retention schedule.

Mitigation: This risk is partially mitigated. USCIS is developing a retention schedule for myUSCIS Account Experience and will not delete records until a retention schedule is approved by NARA. The proposed NARA schedule is consistent with the concept of retaining data only for as long as necessary to support USCIS mission. Until USCIS completes a NARA-approved retention schedule, USCIS plans to maintain all records indefinitely in accordance with the Federal Records Act, which prohibits agencies from destroying records without a NARA-approved schedule.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

USCIS does not share information maintained in myUSCIS Account Experience with external entities. While using myUSCIS Account Experience account holders may engage with third-party service providers, but USCIS does not share PII with third party service providers.

Third Party Authentication Service

myUSCIS Account Experience requires account holders to go through a two-step verification process. As part of two factor authentication, myUSCIS Account Experience account holders are able to use their email, SMS, or third party authentication service provider for the delivery of their two factor authentication code. The selection and use of a third-party authentication application is at the discretion of the account holder. USCIS has no control over the



Homeland Security

Privacy Impact Assessment

DHS/USCIS/PIA-071

myUSCIS Account Experience

Page 19

application's privacy policies or what information the account holder provides.

myUSCIS Account Experience allows individuals to use a third-party authenticator application to provide two-factor authentication into their USCIS online account. ICAM generates a QR code and the account holder must either scan a QR code or enter a unique token manually generated by ICAM using a mobile device to pair the USCIS account with the specific authenticator application. The authenticator service provider then generates a temporary one-time password, which expires every 30 seconds. The temporary one-time password displayed on the account holder's mobile device must be entered into the ICAM system as a second level of authentication upon login. During this transaction, USCIS does not share any PII with the third party authentication service provider.

Pay.Gov

Account holders electronically filing a benefit request form or service must pay for the associated fees using the using the U.S. Department of Treasury's Pay.Gov service.¹⁷ The Pay.Gov icon is imbedded within the digital forms module. Once the account holder clicks the icon, the account holder is redirected to a Pay.Gov, which is a third-party website, to make the fee payment. MyUSCIS Account Experience provides a disclaimer notifying the account holder that he or she is being redirected to a non-USCIS site and is then no longer engaging with myUSCIS. Once an account holder links to Pay.Gov, the account holder is subject to the policies of the third-party site.

Pay.Gov allows account holders to make electronic payments to USCIS. Pay.Gov collects biographic and payment information—either credit card, debit card, or Automated Clearing House (ACH) debit from a personal bank account. Once Pay.Gov validates the payment information, account holders are routed back to myUSCIS Account Experience and the USCIS online account confirms to the account holder that he or she successfully submitted the request. During this transaction, myUSCIS Account Experience does not collect or share any information with Pay.Gov.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

USCIS does not share information maintained in myUSCIS Account Experience with external entities.

6.3 Does the project place limitations on re-dissemination?

USCIS does not share information maintained in myUSCIS Account Experience with external entities.

¹⁷ See U.S. Department of Treasury *Financial Management Services Pay.Gov Privacy Impact Assessment 2.0* (July 1, 2011), available at, http://fms.treas.gov/pia/paygov_pia%20.pdf.



6.4 Describe how the project maintains a record of any disclosures outside of the Department.

USCIS does not share information maintained in myUSCIS Account Experience with external entities.

6.5 Privacy Impact Analysis: Related to Information Sharing

There is no privacy impact related to external information sharing because information maintained in myUSCIS Account Experience is not shared with external entities.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

MyUSCIS Account Experience allows account holders to directly and securely engage with USCIS to obtain useful immigration on case-related information. Account holders who created online accounts must authenticate their identity using the username, password, and authentication code. Once authenticated, individuals may access the information they used to create their profiles, such as name and address information, as well as the case specific information prior to official submission to USCIS.

Additionally, an account holder seeking access to his or her information held by USCIS may gain access to his or her records by filing a Freedom of Information Act (FOIA) or Privacy Act request. Account holders not covered by the Privacy Act or Judicial Redress Act (JRA) still may obtain access to records consistent with FOIA unless disclosure is prohibited by law or if the agency reasonably foresees that disclosure would harm an interest protected by an exemption. Any account holder seeking access to his or her information should direct their request to the following address:

USCIS National Records Center (NRC)
 FOIA/PA Office
 P.O. Box 648010
 Lee's Summit, MO 64064-8010

Further information for Privacy Act and FOIA requests for USCIS records can also be found at <http://www.uscis.gov>.



7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

MyUSCIS Account Experience allows account holders to directly and securely engage with USCIS. Account holders are able to amend information in their accounts by logging in and making the correction to the information they provided prior to official submission to USCIS.

U.S. citizens and lawful permanent residents, as well as other persons with records covered by JRA, are afforded the ability to correct information by filing a Privacy Act Amendment request under the Privacy Act. U.S. citizens, lawful permanent residents, and persons covered by the JRA should submit requests to contest or amend information contained in USCIS systems. Individuals may direct all requests to contest or amend information to the USCIS FOIA/PA Office. Individuals must state clearly and concisely in the redress request the information being contested, the reason for contesting it, the proposed amendment, and clearly mark the envelope "Privacy Act Amendment." This would only apply to amendment of USCIS-held information. Persons not covered by the Privacy Act are not able to amend their records through FOIA. Should a non-U.S. person find inaccurate information in his or her record received through FOIA, he or she may visit a local USCIS Field Office to identify and amend inaccurate records with evidence.

7.3 How does the project notify individuals about the procedures for correcting their information?

Individuals are notified about procedures for correcting their information by myUSCIS Account Experience, published Privacy Notices in relevant USCIS application instructions, the USCIS website, this PIA, and relevant SORNs.

7.4 Privacy Impact Analysis: Related to Redress

There is no privacy risk with respect to redress. Account holders may access the information they enter into myUSCIS Account Experience prior to submission to USCIS. After information is officially submitted to USCIS, USCIS provides individuals with multiple avenues during and after the completion of the benefit request process to correct information. Individuals are also given numerous opportunities to correct information they have provided and to respond to information received from other sources.



Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

USCIS ensures that the practices stated in this PIA are followed by leveraging training, policies, rules of behavior, and auditing and accountability. USCIS established access and security controls to mitigate privacy risks associated with authorized and unauthorized uses, namely misuse and inappropriate dissemination of data. DHS security specifications require auditing capabilities that log the transactions of user in order to reduce the possibility of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify audit information by user identification, network terminal identification, date, time, and data accessed. All USCIS systems employ auditing measures and technical safeguards to prevent the misuse of data.

8.2 Describe what privacy training is provided to account holders either generally or specifically relevant to the project.

All USCIS federal employees and contractors are required to complete annual privacy and security awareness training. The privacy awareness training addresses appropriate privacy concerns, including Privacy Act obligations (e.g., SORN and Privacy Notices). The computer security awareness training examines appropriate technical, physical, personnel and administrative controls to safeguard information.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

MyUSCIS Account Experience is a public-facing website and accessible to any individual or legal representative seeking immigration or case-related information. Account holders have access to their information only. Internal access to myUSCIS Account Experience is restricted by USCIS management and limited to authorized USCIS and contractor personnel.



Homeland Security

Privacy Impact Assessment

DHS/USCIS/PIA-071

myUSCIS Account Experience

Page 23

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

USCIS does not share information maintained in myUSCIS Account Experience with organizations within or outside of DHS. However, should this change, USCIS has a formal review and approval process in place that requires approval of any new sharing arrangement.

Responsible Officials

Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
Department of Homeland Security

Approval Signature

Original, signed copy on file with DHS

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security



**Homeland
Security**

Privacy Impact Assessment

DHS/USCIS/PIA-071

myUSCIS Account Experience

Page 24

Appendix A

Immigration Service Types Filed Online Through myUSCIS

Name of Immigration Service	OMB Control Number
USCIS Immigrant Visa Fee	1615-0122


Appendix B
Immigration Forms Filed Online Through myUSCIS¹⁸

Form Number	Form Name	OMB Control Number
<u>G-28</u>	Notice of Entry of Appearance as Attorney or Accredited Representative	1615-0105
<u>I-90</u>	Replacement of Permanent Resident Card	1615-0082
<u>N-400</u>	Application for Naturalization	1615-0052
<u>N-336</u>	Request for a Hearing on a Decision in Naturalization Proceedings (Under Section 336 of the INA)	1615-0050
<u>N-565</u>	Application for Replacement Naturalization/Citizenship Document	1615-0091

¹⁸ All USCIS Forms are available at <https://www.uscis.gov/forms>.

Mulligan, George D.
 Murphy, Brian J.
 Murray, James M.
 Muzyka, Carolyn L.
 Nally, Kevin J.
 Nelson, Mickey
 Neufeld, Donald W.
 Neumann, Elizabeth
 Neumeister, James
 Nevano, Gregory C.
 Newsome III, Leonza
 Nuebel Kovarik, Kathy
 Nunan, Joanna M.
 Ondocin, Michael A.
 Owen, Todd C.
 Padilla, Kenneth
 Palmer, David J.
 Paramore, Faron K.
 Parker, Debra F.
 Paschall, Robert D.
 Patel, Kalpesh A.
 Patterson, Leonard E.
 Paul, Kshemendra
 Perazzo, Stephen F.
 Perez, Nelson
 Perez, Robert E.
 Perryman, Janet J.
 Piccone, Colleen C.
 Pietropaoli, Lori A.
 Pineiro, Marlen
 Podonsky, Glenn S.
 Pohlman, Teresa R.
 Porto, Victoria
 Price, Corey A.
 Prince, David A.
 Prosnitz, Susan M.
 Provost, Carla L.
 Quinn, Cameron
 Rabin, John L.
 Raymond, John J.
 Renaud, Daniel M.
 Renaud, Tracy L.
 Rexrode, Kathryn S.
 Richardson, Gregory A.
 Ries, Lora L.
 Riordan, Denis C.
 Robbins, Timothy S.
 Robinson, Terri A.
 Rodi III, Louis A.
 Rodriguez, Waldemar
 Roessler, John E.
 Rogers, Debra A.
 Roncone, Stephen A.
 Rosenberg, Ronald M.
 Rosenblum, Marc R.
 Roth, Aaron E.
 Roy, Donna M.
 Ruppel, Joanna
 Rynes, Joel C.
 Sahakian, Diane V.
 Salazar, Rebecca A.
 Salazar, Ronald M.
 Saltalamachea, Michael
 Salvano-Dunn, Dana
 Saunders, Ian C.
 Scott, Kika M.
 Selby, Cara M.
 Sellers, Frederick E.
 Sevier, Adrian
 Seymour, Donna K.
 Shah, Dimple
 Shaw, David C.
 Short, Tracy L.
 Short, Victoria D.
 Sibley, Matthew W.
 Sloan, Terry G.

Smislova, Melissa
 Smith, Brenda B.
 Smith, Frederick B.
 Smith, Stewart D.
 Spero, James
 Spradlin, Ryan L.
 Staton, Jack P.
 Stephens, Celisa M.
 Stiefel, Nathaniel I.
 Stough, Michael S.
 Sulc, Brian
 Sutherland, Dan W.
 Swain, Donald R.
 Swartz, Neal J.
 Sykes, Gwendolyn
 Taylor, Clothilda
 Taylor, Robin M.
 Teeple, Brian
 Thompson, John E.
 Thompson, Kirt
 Tomney, Christopher J.
 Travis, Matthew K.
 Ulrich II, Dennis A.
 Valverde, Michael
 Van Houten, Ann
 Velarde, Barbara Q.
 Venture, Veronica
 Villanueva, Raymond
 Wade, David S.
 Wagner, John P.
 Wallen, Steven
 Walters, Thomas J.
 Walton, Kimberly H.
 Ware, Bryan S.
 Wasowicz, John A.
 Watkins, Tracey
 Watson, Andre R.
 Whalen, Mary Kate
 Wheaton, Kelly D.
 Whittenburg, Cynthia F.
 Wolf, Chad
 Wong, Ricardo A.
 Wong, Sharon M.
 Wonnenberg, David
 Wright, Christopher J.
 Wuco, Frank
 Yarwood, Susan A.
 Young, Edward E.
 Zangardi, John A.
 Zuckowski, Laura B.

Dated: October 2, 2019.

Greg Ruocco,
*Manager, Executive Resources Policy, Office
 of the Chief Human Capital Officer.*
 [FR Doc. 2019-22155 Filed 10-9-19; 8:45 am]

BILLING CODE 9112-FC-P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2019-0042]

Privacy Act of 1974; System of Records

AGENCY: U.S. Citizenship and Immigration Services, Department of Homeland Security.

ACTION: Notice of a Modified System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of

Homeland Security (DHS) proposes to modify and reissue a current DHS system of records titled, "DHS/U.S. Citizenship and Immigration Services (USCIS)-007 Benefits Information System." This system of records describes DHS/USCIS collection, maintenance, processing, and adjudication of naturalization, lawful permanent residence, and other immigrant and nonimmigrant immigration-related requests (hereinafter collectively referred to as "immigration requests") submitted to USCIS in accordance with U.S. immigration law. DHS/USCIS also uses the records contained in the Benefits Information System (BIS) to prevent individuals from fraudulently obtaining immigration and naturalization benefits and to deny immigration and naturalization requests submitted by individuals who pose national security or public safety threats. The BIS may also be used in support of employee performance and production reporting purposes, as well as track an employee or contractor's workload and efficiency in processing a particular immigration request, managing workloads, and providing statistical analyses to USCIS leadership.

DATES: Submit comments on or before November 12, 2019. This modified system will be effective upon publication. New or modified routine uses will be effective November 12, 2019.

ADDRESSES: You may submit comments, identified by docket number DHS-2019-0042 by one of the following methods:

- *Federal e-Rulemaking Portal:* <http://www.regulations.gov>. Follow the instructions for submitting comments.
- *Fax:* 202-343-4010.
- *Mail:* Jonathan R. Cantor, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528-0655.

Instructions: All submissions received must include the agency name and docket number DHS-2019-0042. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Donald K. Hawkins, (202) 272-8030, uscis.privacycompliance@uscis.dhs.gov, Privacy Officer, U.S. Citizenship and Immigration Services, 20 Massachusetts

Avenue NW, Washington, DC 20529. For privacy questions, please contact: Jonathan R. Cantor, (202) 343-1717, Privacy@hq.dhs.gov, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS) U.S. Citizenship and Immigration Services (USCIS) proposes to modify and reissue a current DHS system of records titled, “DHS/USCIS-007 Benefits Information System.”

DHS/USCIS oversees lawful immigration and non-immigration to the United States and is responsible for the administration of immigration, non-immigration, and naturalization adjudication functions and for establishing many immigration policies and priorities. In executing its mission, DHS/USCIS performs functions that include the intake, review, and adjudication of the following types of benefits:

- (1) Family-Based;
- (2) Employment-Based;
- (3) Humanitarian-Based;
- (4) Adoption-Based; and
- (5) Citizenship and Naturalization-Based.

The BIS System of Records Notice (SORN) covers the processing of immigrant and nonimmigrant immigration-related requests.¹ The Secretary of Homeland Security also has the discretion to review and grant other types of immigration requests.² The BIS SORN is specific to USCIS’s collection, use, maintenance, dissemination, and storage of immigration-related request information, including case processing and decisional data.³ USCIS records case processing information, such as date the immigration related request was filed or received by USCIS, request status, location of record, other control number (when applicable), fee receipt data, status of USCIS appointments and interviews, date of issuance of a notice,

¹ This SORN covers all immigrant and nonimmigrant benefit requests, with the exception of requests for asylum, refugee, and intercountry adoption.

² For example, USCIS reviews applications for Deferred Action. Deferred Action is a discretionary determination to defer a deportation of an individual as an act of prosecutorial discretion. Deferred Action can be granted by USCIS or a federal immigration judge.

³ The Immigration Biometric Background Check SORN covers the background check process, while the Benefits Information System SORN covers the storage of background check results. See 83 FR 36950 (July 31, 2018).

and whether the request form was referred to the Fraud Detection and National Security Directorate for review. Decisional data such as an approval/denial code is also stored in BIS. Information within BIS may also be stored in an immigration file (such as an Alien File).⁴

DHS/USCIS is publishing this modified system of records notice to make several changes for transparency and to describe new initiatives. The purpose of this SORN has been expanded to track an employee or contractor’s workload and efficiency in processing a particular benefit request, managing workloads, and providing statistical analyses to USCIS leadership.

The categories of individuals covered by this SORN has been expanded to include prospective accredited representatives seeking to be recognized by the Board of Immigration Appeals, as well as add a new category to cover the collection, maintenance, and use of obligors (surety) and their agents.

New categories of records have been added relating to immigration requestors, which includes country of residence; credit scores and reports; public benefit application, receipt, and certification for receipt information; publicly available social media information and other publicly available information, which may be collected during the course of the benefit adjudication process. New categories of records have been added relating to attorneys and current and/or prospective representatives, which includes USCIS Online Account Number, other identifying numbers (e.g., Attorney Bar Number or equivalent), educational and training history, work history and qualifications, academic and professional achievements, and letters of recommendations. New categories of records have been added relating to bond obligors and their agents including name, identification number(s), contact information (including address, telephone number, email address), signature, and power of attorney. Biometric information and background check results have been removed from remove existing categories of records relating to immigration requestors, derivatives, and family members because they are covered under DHS/

⁴ The Alien File or A-File is the official record regarding the transactions of an individual as he or she passes through the U.S. immigration and inspection process. The Alien File contains information relating to immigration benefits processing, protection of national security, and administering and enforcing immigration and nationality laws and related statutes.

USCIS-018 Immigration Biometric and Background Check SORN.

DHS/USCIS-017 Refugee Case Processing and Security Screening Information SORN and DHS/USCIS-018 Immigration Biometric and Background Check SORN have been added as record source categories, and DHS/USCIS-002 Background Check Service SORN and DHS/USCIS-003 Biometric Storage System SORN have been removed as record source categories.

The routine use section of this SORN has been modified, including updating Routine Use E and adding Routine Use F to comply with requirements set forth by OMB Memorandum M-17-12, “Preparing for and Responding to a Breach of Personally Identifiable Information,” (Jan. 3, 2017); expanding Routine Use V to cover the sharing of information with the petitioning employers to aid in the approval or denial of request to become a permanent resident; updating Routine Use Z to replace Immigration Judge with Federal Judge; adding Routine Use BB for disclosure to government agencies for the purposes of testing new technology; adding Routine Use CC for disclosure to federal, state, local, and tribal public benefit granting agencies to ascertain whether public benefits have been issued to the benefit requestor; adding Routine Use DD for the disclosure to an individual or entity seeking to post or arrange bond; and adding Routine Use EE for the disclosure of petition outcomes to labor unions in instances in which USCIS approves or denies a petition submitted with a union consultation.

Finally, the retention schedules have been modified to reflect disposition schedule by form type and actions, and expand the retention of data in certain case management systems to up to 50 years.

Consistent with DHS’s information sharing mission, information stored in DHS/USCIS-007 Benefits Information System may be shared with other DHS Components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS/USCIS may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice.

Further, specifically, USCIS may share BIS information with DHS’s U.S. Immigration and Customs Enforcement (ICE) Financial Operations—Burlington regarding fees charged during the various immigration requests processes

to ensure collection of debts. The primary mission of the ICE Financial Operations—Burlington is to collect debts resulting from an individual's participation in DHS benefits programs. As such, through DHS's ICE Financial Operations—Burlington office, BIS information may be shared with credit reporting agencies.

This modified system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, the Judicial Redress Act (JRA) provides covered persons with a statutory right to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the DHS/USCIS-007 Benefits Information System System of Records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

SYSTEM NAME AND NUMBER:

Department of Homeland Security (DHS)/U.S. Citizenship and Immigration Services (USCIS)-007 Benefits Information System.

SECURITY CLASSIFICATION:

Unclassified and Classified.

SYSTEM LOCATION:

Records are maintained at the U.S. Citizenship and Immigration Services Headquarters in Washington, DC, and DHS/USCIS service centers and domestic and international field offices. Records are also maintained in DHS/USCIS information technology (IT) systems (e.g., Computer Linked Application Information Management

System (CLAIMS) 3, USCIS Electronic Immigration System (ELIS), Case and Activity Management for International Operations (CAMINO)).

SYSTEM MANAGER(S):

Chief, Immigration Records and Identity Services, Identity and Information Management Division (IIMD), fieldrequests@uscis.dhs.gov, U.S. Citizenship and Immigration Services, Department of Homeland Security, 20 Massachusetts Avenue NW, Washington, DC 20529.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Sections 103 and 290 of the Immigration and Nationality Act, as amended (8 U.S.C. secs. 1103 and 1360), the regulations issued pursuant thereto; and Section 451 of the Homeland Security Act of 2002 (Pub. L. 107-296).

PURPOSE(S) OF THE SYSTEM:

The purpose of this system is to permit USCIS's collection, use, maintenance, dissemination, and storage of paper and electronic immigration-related request information, including case processing and decisional data. These records assist in the processing of immigrant and nonimmigrant benefit requests and other immigration-related requests from the time when USCIS collects the information from the immigration-related requestor until the case receives a final decision in the relevant case management system.⁵ This system of records enables DHS/USCIS to process benefit requests electronically, determine the status of pending benefit requests, account for and control the receipt and disposition of any fees and refunds collected, conduct searches pursuant to requests under the Freedom of Information Act (FOIA) and Privacy Act, and locate related physical and automated files to support DHS/USCIS responses to inquiries about these records. This system of records may also be used in support of monitoring employee performance and production reporting purposes, including tracking an employee or contractor's workload and efficiency in processing a particular benefit request, managing workloads, and providing statistical analyses to USCIS leadership.

DHS/USCIS maintains a replica of some or all of the data in application databases on DHS unclassified and classified networks to allow for analysis and vetting consistent with the above stated purposes and this published notice.

⁵ This system of records does not cover requests for intercountry adoption, asylum, or refugee status.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include (1) individuals who have filed, for themselves or on the behalf of others (benefit requestors and beneficiaries and other immigration-related requestors), requests for immigration benefits and other requests under the Immigration and Nationality Act as amended, and/or who have submitted fee payments or received refunds from such requests; (2) current, former, and potential derivatives of requestors (family members); (3) sponsors (e.g., employers, law enforcement officers, or other individuals); (4) attorneys; (5) prospective representatives seeking recognition from and current accredited representatives recognized by USCIS and/or by the Board of Immigration Appeals (Representatives); (6) interpreters; (7) individuals who assist in the preparation of the immigration-related request forms (Preparers); (8) individuals who make fee payments on behalf of the immigration-related requestor; (9) physicians who conduct immigration-related medical examinations; and (10) obligors (surety) and their agents.

CATEGORIES OF RECORDS IN THE SYSTEM:

Information about benefit requestors, beneficiaries, and family members may include:

- Full name;
- Alias(es);
- Physical, destination, and mailing addresses (including foreign and domestic);
- Unique Identifying Numbers (e.g., Alien Number, USCIS Online Account Number, Social Security number (SSN), and Data Universal Numbering System (DUNS) Number);
- Date of birth and/or death;
- Nationality and/or Place of Birth (including city, region, and country of birth);
- Country or countries of citizenship;
- Country of Residence;
- Gender and/or sex;
- Marital status;
- Military status;
- Phone and fax numbers;
- Email address;
- Immigration status;
- Publicly available social media information and information from public-facing websites;
- Responses to questions on immigration benefit forms (e.g., have you ever claimed to be a U.S. citizen; do you owe any federal, state, or local taxes)
- Government-issued identification (e.g., passports, driver's license, national ID);

- Document type;
- Issuing country and/or organization;
- Document number;
- Issue Date;
- Expiration date;
- Notices and communications, including:
 - Receipt notices;
 - Requests for Evidence;
 - Notices of Intent to Deny;
 - Proofs of benefit;
 - Type of benefit requested;
 - Signature (wet and digital);
 - Immigration-related request fee payment information (e.g., credit card number, *Pay.gov* Payment Tracking Number); and
 - Audio-visual recordings, including interviews and naturalization ceremonies.
- Benefit-specific eligibility information about benefit requestor, beneficiaries, and family members may include:
 - Other unique identifying numbers (e.g., Department of State (DOS)-Issued Personal Identification Number, ICE Student and Exchange Visitor Number, USCIS E-Verify Company Identification Number);
 - Arrival/Departure Information;
 - Immigration history (e.g., citizenship/naturalization certificate number, apprehensions, removals, explanations);
 - Familial relationships (e.g., parent, spouse, sibling, child, other dependents);
 - Relationship Practices (e.g., polygamy, custody, guardianship);
 - USCIS Receipt/Case Number;
 - Personal background information (e.g., involvement with national security threats; criminal offenses; Communist Party membership; participation in torture, genocide, killing, injuring, forced sexual contact, limiting or denying others religious beliefs, weapons distribution, or combat training; service in military or other armed groups, work in penal or detention systems);
 - Records regarding organization membership or affiliation;
 - Health information (e.g., vaccinations, referrals, communicable diseases, physical or mental disorders or disabilities, prostitution, drug or alcohol abuse);
 - Travel history;
 - Education history;
 - Employment history;
 - Professional accreditation information;
 - Financial information (e.g., credit scores and reports, income, expenses, scholarships, savings, assets, property, financial support, supporter information, life insurance, debts, encumbrances, and tax records);

- Public benefit information (e.g., applications and receipt, as well as certification of receipt of public benefits);
 - Supporting documentation as necessary (e.g., birth, marriage, and divorce certificates; licenses; academic diplomas; academic transcripts; appeals or motions to reopen or reconsider decisions; explanatory statements; deoxyribonucleic acid (DNA) results; and unsolicited information submitted voluntarily by the benefit requestor or family members in support of a benefit request);
 - Physical description (e.g., height, weight, eye color, hair color, race, ethnicity, identifying marks like tattoos or birthmarks);
 - Description of relationships between benefit requestors, representatives, preparers, and family members;
 - Information regarding the status of Department of Justice (DOJ), Executive Office of Immigration Review (EOIR) proceedings, if applicable; and
 - Case processing information such as date benefit requests were filed or received by USCIS, benefit request status, location of record, other control number when applicable, and fee receipt data.
- Information about Benefit Sponsors may include:
 - Full name;
 - Gender and/or sex;
 - Physical and mailing addresses;
 - Phone and fax numbers;
 - Country of domicile;
 - Date of birth;
 - Place of birth;
 - Citizenship information;
 - SSN;
 - A-Number;
 - USCIS Online Account Number;
 - Employment information;
 - Financial information (e.g., income, expenses, scholarships, savings, assets, property, financial support, supporter information, life insurance, debts, encumbrances, tax records);
 - Position and relationship to an organization (e.g., manager of a company seeking formal recognition by USCIS);
 - Family relationships (e.g., parent, spouse, sibling, natural, foster, and/or adopted child, other dependents); and
 - Relationship practices (e.g., polygamy, custody, guardianship).
- Information about Attorneys and current and/or prospective Accredited Representatives include:
 - Name;
 - USCIS Online Account Number
 - Other identifying numbers (e.g., Attorney Bar Card Number or equivalent);
 - Law firm/recognized organization;

- Physical and mailing addresses;
- Phone and fax numbers;
- Email address;
- Bar membership and Bar number;
- Accreditation date;
- Board of Immigration Appeals Representative Accreditation;
 - Expiration date;
 - Law Practice Restriction explanation;
 - Educational and training history;
 - Work history and qualifications;
 - Academic and professional achievements;
 - Letters of recommendation; and
 - Signature.
- Information about Preparers and Interpreters may include:
 - Full name;
 - Organization;
 - Business State ID number;
 - Employer Tax Identification Number;
 - Physical and mailing addresses;
 - Email address;
 - Phone and fax numbers;
 - Relationship to benefit requestor; and
 - Signature.
- Information about individuals who make fee payments on behalf of the immigration-related requestor includes:
 - Name;
 - Email address;
 - Phone number;
 - Mailing address; and
 - Payment information.
- Information about Physicians may include:
 - Full name;
 - Organization name;
 - Physical and mailing addresses;
 - Phone number;
 - Fax number;
 - Professional experience;
 - License number;
 - Other Physician Identifying Number(s);
 - Licensing state and date of issuance;
 - Type of degree/license (such as medical doctor, doctor of osteopathy, or clinical psychologist);
 - Type of medical practice;
 - Examination dates of the benefit requestor;
 - Clinical methods used to diagnose benefit requestor;
 - Email address; and
 - Signature.
- Information about obligor (surety) and its agents (co-obligor) may include:
 - Name;
 - Unique Identifying Number (e.g., Taxpayer Identification Number (TIN), Employer Identification Number (EIN), SSN (in some cases, the obligor's TIN or EIN may be the individual's SSN, and DUNS Number));

- Address (Street, City, State and Zip Code);
- Telephone Number;
- Email Address;
- Power of Attorney (evidencing authority to act on behalf of the surety) and Power of Attorney number;
- Signature; and
- Information about bond (e.g., receipt number and bond amount).

RECORD SOURCE CATEGORIES:

DHS/USCIS obtains records from the immigration requestor, his or her Representative, Physician, Preparer, Interpreter, or obligor and its agents. DHS/USCIS personnel may input information as they process a case, including information from internal and external sources to verify whether a requestor or family member is eligible for the immigration-related request. BIS also stores and uses information from the following USCIS, DHS, and other federal agency systems of records:

- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, September 18, 2017 (82 FR 43556);
- DHS/USCIS-005 Inter-Country Adoptions, November 8, 2016 (81 FR 78614);
- DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), August 8, 2012 (77 FR 47411);
- DHS/USCIS-010 Asylum Information and Pre-Screening System of Records, November 30, 2015 (80 FR 74781);
- DHS/USCIS-017 Refugee Case Processing and Security Screening Information System of Records, October 19, 2016 (81 FR 72075);
- DHS/USCIS-018 Immigration Biometric and Background Check Records System of Records, July 31, 2018 (83 FR 36950);
- DHS/CBP-011 U.S. Customs and Border Protection TECS, December 19, 2008 (73 FR 77778);
- DHS/ICE-001 Student and Exchange Visitor Information System, January 5, 2010 (75 FR 412);
- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), October 19, 2016 (81 FR 72080);
- DHS/CBP-021 Arrival and Departure Information System (ADIS), November 18, 2015 (80 FR 72081);
- JUSTICE/EOIR-001 Records and Management Information System, January 25, 2007 (72 FR 3410);
- JUSTICE/FBI-002 The FBI Central Records System, January 25, 2007 (72 FR 3410);
- JUSTICE/FBI-009 Fingerprint Identification Records System (FIRS), January 25, 2007 (72 FR 3410);

- DOL/ETA-7 Employer Application and Attestation File for Permanent and Temporary Alien Workers, January 10, 2012 (77 FR 1728);
- STATE-05 Overseas Citizens Services Records, May 2, 2008 (73 FR 24343);
- STATE-26 Passport Records, July 6, 2011 (76 FR 34966);
- STATE-39 Visa Records, October 25, 2012 (77 FR 65245); and
- TREASURY/FMS-017 Collections Records, May 15, 2009 (74 FR 23006).

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

Information in this system of records contains information relating to individuals who received benefit requests for special protected classes and should not be disclosed pursuant to a routine use unless disclosure is otherwise permissible under the confidentiality statutes, regulations, or policies applicable to that information. For example, information relating to individuals who received benefit requests for protection under the Violence Against Women Act, Seasonal Agricultural Worker or Legalization claims, the Temporary Protected Status of an individual, and information relating to nonimmigrant visas protected under special confidentiality provisions should not be disclosed pursuant to a routine use unless disclosure is otherwise permissible under the confidentiality statutes, regulations, or policies applicable to that information. These confidentiality provisions do not prevent DHS from disclosing information to the DOJ and U.S. Attorneys Offices as part of an ongoing criminal or civil investigation.

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To DOJ, including the U.S. Attorney's Offices, or other federal agencies conducting litigation or proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation or proceeding and one of the following is a party to the litigation or proceeding or has an interest in such litigation or proceeding:

1. DHS or any component thereof;
2. Any employee or former employee of DHS in his/her official capacity;
3. Any employee or former employee of DHS in his/her individual capacity, only when DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. secs. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when (1) DHS suspects or has confirmed that there has been a breach of the system of records; (2) DHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DHS (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

F. To another federal agency or federal entity, when DHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

G. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations, and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative

agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

I. To clerks and judges of courts exercising naturalization jurisdiction for the purpose of filing applications for naturalization and to enable such courts to determine eligibility for naturalization or grounds for revocation of naturalization.

J. To the Department of State for the purpose of assisting in the processing of benefit requests under the Immigration and Nationality Act, and all other immigration and nationality laws including treaties and reciprocal agreements.

K. To appropriate federal, state, tribal, and local government law enforcement and regulatory agencies, foreign governments, and international organizations, as well as to other individuals and organizations during the course of an investigation by DHS or the processing of a matter under DHS jurisdiction, or during a proceeding within the purview of the immigration and nationality laws, when DHS deems that such disclosure is necessary to carry out its functions and statutory mandates to elicit information required by DHS to carry out its functions and statutory mandates.

L. To an appropriate federal, state, local, tribal, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual; issuance of a security clearance, license, contract, grant, or other benefit; or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit and when such disclosure is appropriate to the proper performance of the official duties of the person making the request.

M. To the Office of Management and Budget in connection with the review of private relief legislation as set forth in OMB Circular No. A-19 at any stage of the legislative coordination and clearance process as set forth in the Circular.

N. To an attorney or representative (as defined in 8 CFR 1.1(j)) who is acting on behalf of an individual covered by this system of records in connection with any proceeding before DHS/USCIS or

the DOJ Executive Office for Immigration Review.

O. To a federal, state, tribal, or local government agency to assist such agencies in collecting the repayment of loans, fraudulently or erroneously secured benefits, grants, or other debts owed to them or to the U.S. Government, or to obtain information that may assist USCIS in collecting debts owed to the U.S. Government;

P. To a foreign government to assist such government in collecting the repayment of loans, fraudulently or erroneously secured benefits, grants, or other debts owed to it, provided that the foreign government in question:

1. Provides sufficient documentation to establish the validity of the stated purpose of its request; and

2. Provides similar information to the United States upon request.

Q. To a coroner for purposes of affirmatively identifying a deceased individual (whether or not such individual is deceased as a result of a crime).

R. Consistent with the requirements of the Immigration and Nationality Act, to the Department of Health and Human Services (HHS), the Centers for Disease Control and Prevention (CDC), or to any state or local health authorities, to:

1. Provide proper medical oversight of DHS-designated civil surgeons who perform medical examinations of both arriving foreign nationals and of those requesting status as a lawful permanent resident; and

2. To ensure that all health issues potentially affecting public health and safety in the United States are being, or have been, adequately addressed.

S. To a federal, state, or local government agency seeking to verify or ascertain the citizenship or immigration status of any individual within the jurisdiction of the agency for any purpose authorized by law.

T. To the Social Security Administration (SSA) for the purpose of issuing a Social Security number and card to an alien who has made a request for a Social Security number as part of the immigration process and in accordance with any related agreements in effect between the SSA, DHS, and the Department of State entered into pursuant to 20 CFR 422.103(b)(3); 422.103(c); and 422.106(a), or other relevant laws and regulations.

U. To a former employee of DHS, in accordance with applicable regulations, for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority or facilitating communications with a former employee that may be necessary for

personnel-related or other official purposes when the Department requires information or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

V. To an individual's prospective or current employer to the extent necessary to determine employment eligibility (e.g., pursuant to the Form I-140, *Immigrant Petition for Alien Worker*) or, USCIS may share information with the petitioning employers to aid in the approval or denial of a request to become a permanent resident.

W. To a federal, state, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law or Executive Order.

X. To approved federal, state, and local government agencies that grant public benefits, licenses, grants, governmental credentials, or for any other statutorily authorized purpose when the immigration status of the benefit applicant is legally required and an approved Memorandum of Agreement or Computer Matching Agreement (CMA) is in place between DHS and the entity.

Y. To the Department of Labor for enforcement of labor certification violations and violations of U.S. labor laws.

Z. To the news media and the public during the course of naturalization ceremonies administered by USCIS or a Federal Judge. Pursuant to 8 CFR 337.2 individuals to be naturalized are generally required to appear in a public ceremony, unless an appearance is specifically excused.

AA. To the Department of Treasury to perform initial processing of benefit requests and to accept and resolve payment and any related issues.

BB. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, with the approval of the Chief Privacy Officer, when DHS is aware of a need to use relevant data, that relate to the purpose(s) stated in this SORN, for purposes of testing new technology.

CC. To federal, state, local, and tribal benefit granting agencies (e.g., Social Security, housing, food, unemployment) to ascertain whether public benefits have been issued to the immigration requestor.

DD. To an individual or entity seeking to post or arrange, or who has already

posted or arranged, an immigration bond for an alien, to aid the individual or entity in (1) identifying the location of the alien; (2) posting the bond; (3) obtaining payments related to the bond; or (4) conducting other administrative or financial management activities related to the bond.

EE. To a consulting entity (e.g., a labor organization or management organization) that provided an advisory opinion on a petition to USCIS seeking O or P nonimmigrant classification. USCIS may disclose the outcome of the petition to the consulting entity that provided an advisory opinion on the petition.

FF. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information; when disclosure is necessary to preserve confidence in the integrity of DHS; or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute a clearly unwarranted invasion of personal privacy.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

DHS/USCIS stores records in this system electronically or on paper in secure facilities, such as in a locked drawer or behind a locked door. The records may also be stored on magnetic disc, tape, and digital media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

DHS/USCIS may retrieve records by using any of the data elements listed above or a combination thereof. This may include, but is not limited to, name, date of birth, Alien Number, SSN, USCIS Online Account Number, and Receipt Number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

USCIS receives and adjudicates immigration request forms. Each form type is governed by a respective retention schedule and each form type's retention period is dictated by USCIS's final action on the form (e.g., approved, denied, abandoned, withdrawn, administratively closed, and rejected). Immigration request forms and supplemental documentation that constitute the official record of an individual's immigration history are stored in the individual's paper and/or electronic Alien File. The Alien File

records are permanent, whether hard copy or electronic. DHS/USCIS is eligible to transfer Alien Files to the custody of NARA 100 years after the individual's date of birth.

USCIS uses multiple case management systems for the processing, adjudication, and management of paper and electronically filed immigration request forms. Each case management system retains records in accordance with NARA-approved retention schedules. Generally, information is retained between 25–50 years from the last completed action. The duration of the NARA-approved retention schedules allows USCIS to address any follow-up inquiries or requests related to the immigration request form, including inquiries related to law enforcement, public safety, national security, and to FOIA and Privacy Act matters. These retention periods allow USCIS to provide as much information as possible to an individual regarding his or her immigration history.

Electronic notices and communications associated with an immigration request, to include Approval or Denial letters, Requests for Evidence, Notices of Intent to Deny, Appeal/Motion Responses, etc., are retained for 13 years after the last completed action with respect to the benefit.

Records of electronic appointments with USCIS are maintained for 60 days after the date of the appointment.

Daily reports generated by associated information technology systems are maintained in accordance with the general records retention schedule that permits USCIS to destroy reports when no longer needed.

Records replicated on the unclassified and classified networks for analysis and vetting will follow the same retention schedule.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

DHS/USCIS safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. USCIS has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RECORD ACCESS PROCEDURES:

Individuals seeking access to and notification of any record contained in

this system of records, or seeking to contest its content, may submit a request in writing or electronically to the Chief Privacy Officer or USCIS's FOIA Officer, whose contact information can be found at <http://www.dhs.gov/foia> under "Contact Information." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief FOIA Officer, Department of Homeland Security, Washington, DC 20528–0655. Even if neither the Privacy Act nor the Judicial Redress Act provides a right of access, certain records may be available under the FOIA.

When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the individual's request must conform with the Privacy Act regulations set forth in 6 CFR part 5. The individual must first verify his/her identity, meaning that the individual must provide his/her full name, current address, and date and place of birth. The individual must sign the request, and the individual's signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, an individual may obtain forms for this purpose from the Chief Privacy Officer and Chief FOIA Officer, <http://www.dhs.gov/foia> or 1–866–431–0486. In addition, the individual should:

- Explain why he or she believe the Department would have information being requested;
- Identify which component(s) of the Department he or she believe may have the information;
- Specify when the individual believes the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records;

If an individual's request is seeking records pertaining to another living individual, the first individual must include a statement from the second individual certifying that individual's agreement for the first individual to access his/her records.

Without the above information, the component(s) may not be able to conduct an effective search, and the individual's request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES:

For records covered by the Privacy Act or covered JRA records, see "Record Access Procedures" above. Any individual, regardless of immigration status, may file a request to access his or her information under the FOIA. Throughout the benefit determination process, and prior to USCIS making a determination to deny a benefit request, USCIS provides individuals with the opportunity to address and correct the information.

NOTIFICATION PROCEDURES:

See "Record Access Procedures" above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None. However, when this system receives a record from another system exempted under 5 U.S.C. 552a, DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated.

HISTORY:

81 FR 72069 (October 19, 2016); 73 FR 56596 (September 29, 2008).

Jonathan R. Cantor,

Acting Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2019-22156 Filed 10-9-19; 8:45 am]

BILLING CODE 9111-17-P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

[Docket No. FR-7022-N-01]

60-Day Notice of Proposed Information Collection: Opportunity Zone Grant Certification Form

AGENCY: Office of Field Policy and Management, HUD.

ACTION: Notice.

SUMMARY: HUD is seeking approval from the Office of Management and Budget (OMB) for the information collection described below. In accordance with the Paperwork Reduction Act, HUD is requesting comment from all interested parties on the proposed collection of information. The purpose of this notice is to allow for 60 days of public comment.

DATES: *Comments Due Date:* December 9, 2019.

ADDRESSES: Interested persons are invited to submit comments regarding this proposal. Comments should refer to the proposal by name and/or OMB Control Number and should be sent to: Colette Pollard, Reports Management Officer, QDAM, Department of Housing and Urban Development, 451 7th Street SW, Room 4176, Washington, DC 20410-5000; telephone 202-402-3400 (this is not a toll-free number) or email at *Colette.Pollard@hud.gov* for a copy of the proposed forms or other available information. Persons with hearing or speech impairments may access this number through TTY by calling the toll-free Federal Relay Service at (800) 877-8339.

FOR FURTHER INFORMATION CONTACT: Alex Stowe, Advisor, Field Policy and Management, Department of Housing and Urban Development, 451 7th Street SW, Washington, DC 20410; email *alexander.d.stowe@hud.gov* or telephone 202-402-5309. This is not a toll-free number. Persons with hearing or speech impairments may access this number through TTY by calling the toll-free Federal Relay Service at (800) 877-8339. Copies of available documents submitted to OMB may be obtained from Mr. Stowe.

SUPPLEMENTARY INFORMATION: This notice informs the public that HUD is seeking approval from OMB for the information collection described in Section A.

A. Overview of Information Collection

Title of Information Collection: Certification of Consistency With Opportunity Zone Initiative-Related Activity.

OMB Approval Number: 2501-.

Type of Request: New Collection.

Form Number: HUD-XXXX

Certification for Opportunity Zone Preference Points.

Description of the need for the information and proposed use: This collection is a new collection regarding information for preference points in certain competitive federal grants and technical assistance applications. In accordance with Executive Order 13853, Establishing the White House Opportunity and Revitalization Council ("WHORC" or "Council"), signed by

President Trump on December 12, 2018, the Department of Housing and Urban Development (HUD) has added preference points to grants in an effort to strategically target investment in communities designated as Opportunity Zones. To ensure that HUD's resources are being used to further the mission of the Executive Order and the WHORC Implementation Plan (published April 17, 2019), HUD has drafted the proposed certification form. This form will certify that valuable HUD resources are in fact being targeted to and expended in America's most economically distressed areas, including Opportunity Zones. Additionally, it will enable HUD to gather and analyze the most accurate data regarding the use of taxpayer funds; specifically, how they are being utilized by our grantee partners to support the President's mission of revitalizing distressed communities. The collection of this information will help to guide the Department through future grant awards and inform HUD's strategy to maximize non-profit and private sector investment.

Additionally, pending approval of this form on HUD's behalf, we anticipate that the following Agencies will also implement this form: Agriculture, Commerce, Education, Justice, Health and Human Services, Labor, Transportation, Interior, Commerce, Energy, Veterans Affairs, the Small Business Administration and the Environmental Protection Agency. Public and private investment in America's historically overlooked communities will be used to increase the supply of affordable housing to bolster economic development, support entrepreneurship, promote neighborhood safety, and expand employment and educational opportunities. For more information about the mission of the WHORC and to learn about the activities and vision of the federal agencies that comprise the Council, visit <https://www.hud.gov/sites/dfiles/Main/documents/WHORC-Implementation-Plan.pdf>.

Respondents (i.e., *affected public*): HUD grant applicants applying for preference points for activities conducted within or benefiting designated Qualified Opportunity Zone census tracts.

36950

Federal Register / Vol. 83, No. 147 / Tuesday, July 31, 2018 / Notices

determination before the Court of International Trade.

Sincerely,
Alice A. Kipel
Executive Director
Regulations and Rulings
Office of Trade

[FR Doc. 2018-16281 Filed 7-30-18; 8:45 am]

BILLING CODE P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2018-0003]

Privacy Act of 1974; System of Records

AGENCY: Department of Homeland Security.

ACTION: Notice of a new system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to consolidate two legacy systems of record, Department of Homeland Security/U.S. Citizenship and Immigration Services-002 Background Check Service and Department of Homeland Security/U.S. Citizenship and Immigration Services-003 Biometric Storage System into the new DHS system of records titled, “Department of Homeland Security/U.S. Citizenship and Immigration Services-018 Immigration Biometric and Background Check System of Records.” This system of records notice (SORN) allows the DHS U.S. Citizenship and Immigration Services (USCIS) to collect and maintain biographic, biometric, and background check records on applicants, petitioners, sponsors, beneficiaries, or other individuals in connection with a benefit request. USCIS uses biometric and associated biographic information to verify identity, conduct criminal and national security background checks against internal and external government systems, and to support domestic and foreign data sharing agreements. The categories of individuals, categories of records, and the routine uses of these legacy systems of records notices have been consolidated and updated to better reflect the Department’s biometric and biographic criminal background checks; identity enrollment, verification, and resolution; document production record systems; and data sharing efforts.

Additionally, DHS is issuing a Notice of Proposed Rulemaking (NPRM) to exempt this system of records from certain provisions of the Privacy Act, elsewhere in the **Federal Register**. This

new system will be included in DHS’s inventory of record systems.

DATES: Submit comments on or before August 30, 2018. This system will be effective upon publication. Routine uses will become effective August 30, 2018.

ADDRESSES: You may submit comments, identified by docket number DHS-2018-0003 by one of the following methods:

- *Federal e-Rulemaking Portal:* <http://www.regulations.gov>. Follow the instructions for submitting comments.

- *Fax:* 202-343-4010.
- *Mail:* Philip S. Kaplan, Chief

Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528-0655.

Instructions: All submissions received must include the agency name and docket number DHS-2018-0003 for this notice. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Donald K. Hawkins, (202) 272-8030, *USCIS.PrivacyCompliance@uscis.dhs.gov*, Privacy Officer, U.S. Citizenship and Immigration Services, 20 Massachusetts Avenue NW, Washington, DC 20529. For privacy questions, please contact: Philip S. Kaplan, (202) 343-1717, *Privacy@hq.dhs.gov*, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

DHS USCIS has relied on two preexisting DHS/USCIS Privacy Act SORNs for the maintenance of USCIS biometric and background check records: “DHS/USCIS 002 Background Check Service,” 72 FR 31082 (June 5, 2007), and “DHS/USCIS-003 Biometric Storage System,” 72 FR 17172 (April 6, 2007). Such records will be covered by one new system of records named “DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records.” USCIS processes and adjudicates most immigration benefit requests and other immigration request forms (e.g., applications and petitions) for DHS. This new system of records notice consolidates and covers all of USCIS’s biometric and associated biographic information it collects pursuant to that mission. The purpose of this system is to verify identity and conduct criminal and national security

background checks in order to establish an individual’s eligibility for an immigration benefit or other request, and support domestic and international data sharing efforts. USCIS determines eligibility by capturing biometric and associated biographic data from benefit requestors, beneficiaries, and other categories of individuals to facilitate three key operational functions: (1) Verify an individual’s identity; (2) conduct criminal and national security background checks; and (3) produce benefit cards and documents as a proof of benefit.

Most individuals who file benefit requests for themselves or on the behalf of others (i.e., petitioner, applicants, beneficiaries, and requestors) are subject to background, identity, and security checks to ensure eligibility for the requested benefit. Other individuals in connection with immigration benefit requests or other requests (i.e., household members, sponsors) may also be subject to certain background, identity, and security checks. The biometric collection process begins with the capture of biometric data at an authorized biometric capture site, including USCIS offices, Application Support Centers, or U.S. consular offices and military installations abroad. USCIS requires applicants, petitioners, sponsors, beneficiaries, or other individuals in connection of a benefit request to submit their biometrics along with associated biographic information to USCIS for background, identity, and security checks. The types of background checks USCIS conducts vary by the benefit or request type. Standard background checks may include, but are not limited to:

Biometric based checks:

- Federal Bureau of Investigation (FBI) Next Generation Identification (NGI) Biometric Check;
- DHS Office of Biometric and Identity Management (OBIM) Automated Biometric Identification System (IDENT) Biometric Check;
- Department of Defense (DoD) Automated Biometric Identification System (ABIS) Biometric Check;

Biographic name-based checks:

- FBI Central Records System (CRS) and Universal Index (UNI) Name Check;
- U.S. Customs and Border Protection (CBP) TECS Name Checks;
- Department of State (DOS) Consular Lookout and Support System (CLASS); and
- DOS Security Advisory Opinion (SAO).

USCIS may also perform interagency checks with intelligence community partners for certain benefits. The results of these checks are used to inform

eligibility determinations, which will result in the approval or denial of a benefit. If fraudulent activity, criminal activity, or potential threats to public safety or national security are detected as a result of the biometric or name check, information may be referred to the USCIS Fraud Detection and National Security Directorate (FDNS) or appropriate law enforcement agencies for further review. These law enforcement agencies include U.S. Immigration and Customs Enforcement (ICE), CBP, FBI, or other federal, state, local, tribal, foreign, or international law enforcement agencies. USCIS may also conduct additional background and security checks against other federal, international, state, and local systems to verify the identity of the individual as part of the eligibility determination for a benefit or request, as appropriate.

USCIS sends biometric, associated biographic, and encounter-related data to IDENT to conduct biometric searches against the system. IDENT is the central DHS-wide information technology system for enrollment, storage, and processing of biometric and associated biographic information. IDENT is maintained for the purposes of national security, law enforcement, immigration and border management, intelligence, and credentialing (e.g., background investigations for national security positions and certain positions of public trust), as well as for other administrative uses (e.g., providing associated testing, training, management reporting, or planning and analysis). When an authorized request is received by OBIM, the program management office for IDENT, analysts search IDENT for biometric matches and assign matches as new encounters into IDENT on behalf of USCIS. Consistent with this SORN and other SORNS governing different biometric data sets in IDENT, USCIS biographic and biometric information from IDENT may be shared with federal, state, local, tribal, foreign, and international agencies for national security, law enforcement, criminal justice, immigration and border management, and intelligence purposes. In addition, information from IDENT may also be shared for background investigations for national security positions and certain positions of public trust in accordance with statutory and regulatory restrictions on disclosure.

International Biometric Sharing Initiatives

This system of records supports the biometric vetting capability outlined in data sharing agreements between DHS and certain foreign partners. USCIS may send and receive biometric requests to

and from certain foreign partners through IDENT in support of its immigration mission and applicable laws. The purpose of these data sharing initiatives is to enhance the cooperation between the United States and foreign partners to prevent terrorism, including terrorist travel; prevent serious crime and other threats to national security and public safety; assist in the administration and enforcement of immigration laws; and provide the foreign partner with appropriate information for its consideration when adjudicating requests for immigration benefits including, but not limited to, asylum or refugee status. Through international sharing agreements, USCIS may share biometric and associated biographic information stored in IDENT, which it collected in determining suitability for an immigration benefit, with foreign partners. DHS does not permit third party disclosure without prior approval.

Document Production

Once the adjudication of certain immigration benefits are complete, USCIS creates official, personalized and secure identity documents to certify the grant of the requested benefit. The secure identification documents USCIS produces and issues are high-quality and state-of-the-art, incorporating tamper-resistant, machine-readable, and biometrically-enabled technologies designed to withstand document counterfeiting efforts, alteration, or efforts employed to commit fraud.

Information stored in the DHS/USCIS-018 IBBC System of Records may be shared with other DHS Components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS/USCIS may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice.

Additionally, DHS is issuing an NPRM to exempt this system of records from certain provisions of the Privacy Act elsewhere in the **Federal Register**. This new system of records will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework under which Federal Government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act

applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, the Judicial Redress Act (JRA) provides statutory rights to covered persons to request access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the DHS/USCIS-018-Immigration Biometric and Background Check (IBBC) System of Records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

SYSTEM NAME AND NUMBER:

DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records.

SECURITY CLASSIFICATION:

Unclassified and classified. The data may be retained on classified networks but this does not change the nature and character of the data until it is combined with classified information.

SYSTEM LOCATION:

DHS/USCIS maintains records in DHS-approved data centers in the Washington, DC, metropolitan area. Backups are maintained offsite. IBBC will be accessible world-wide from all USCIS field offices, service centers, and Application Service Centers that are part of the DHS Network. Paper files are located at USCIS Headquarters in Washington, DC and in DHS/USCIS service centers, domestic and international field offices, and other USCIS facilities. USCIS stores biometric records in the DHS biometrics repository, OBIM IDENT.

DHS/USCIS replicates records from the operational IT systems and maintains them in other IT systems connected on the DHS unclassified and classified networks.

SYSTEM MANAGER(S):

Associate Director, Immigration Records and Identity Services, BD.systems@uscis.dhs.gov, U.S. Citizenship and Immigration Services,

Department of Homeland Security, 111 Massachusetts Avenue NW, Washington, DC 20529.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

8 U.S.C. 1101 and 1103; 8 CFR 103.16(a); and 8 CFR 103.2(b)(9).

PURPOSE(S) OF THE SYSTEM:

The purpose of this system is to assist USCIS with determining an individual's eligibility for an immigration benefit request or other USCIS requests. USCIS captures biographic and biometric data from applicants, petitioners, sponsors, beneficiaries, or other individuals to facilitate three key operational functions: (1) Enroll, verify, and manage an individual's identity; (2) conduct criminal and national security background checks; and (3) produce benefit cards/documents as a proof of benefit. Also, the purpose of this system is to (4) support data sharing initiatives between DHS components, other U.S. Government agencies and foreign partners in order to prevent terrorism, including terrorist travel; prevent serious crime and other threats to national security and public safety; and assist in the administration and enforcement of immigration laws.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include:

- Persons who have filed on their own behalf, or on the behalf of others, applications or petitions for immigration benefits or other requests under the Immigration and Nationality Act (INA) (i.e., applicants, petitioners, and beneficiaries), as amended;
- Current, former, and potential derivative family members of benefit requestors;
- Affiliated persons who have a clearly articulated rational connection to the request, applicant, petitioner, or beneficiary, that may have an impact on the adjudication process of a request;
- Associates whose information is voluntarily provided by the applicant as part of the family tree, and which include points of contact in the United States and other individuals with whom the applicant associates (i.e., household members, sponsors);
- Attorneys and representatives recognized by USCIS and/or accredited by the Board of Immigration Appeals (Representatives); and
- All individuals who meet the definition of an adult member of the household, 8 CFR 204.3(b) or 8 CFR 204.301; and/or any other individual whose presence in the applicant's or petitioner's residence is relevant to the

prospective adoptive parent(s)'s suitability to adopt overseas.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system covers biographic, biometric, unique machine-generated identifiers, encounter-related data, criminal and national security background check results, and card production information.

Biographic information may include:

- Full name;
- Aliases;
- Other names;
- Date of birth;
- Place of birth;
- Country of Citizenship/Nationality;
- Current and previous immigration status;
- Mailing and physical address;
- Phone number;
- Employment status;
- Travel Document Numbers (i.e., passport numbers, I-94 number);
- Travel Document Information (i.e., country of issuance, nationality, date of issuance, expiration date);
- Case Type (i.e., refugee claimant, identity investigation, absconder, visa applicant);
- Filing date;
- Filing determination;
- Reason for filing determination;
- Gender;
- Height;
- Weight;
- Eye color;
- Hair color;
- Race/Ethnicity; and
- Unique Identifying Numbers, including, but not limited to, Alien Registration Number (Alien Number), Receipt Number, Social Security number (SSN), and USCIS Online Account Number.

Biometric information may include:

- Biometric images (including, but not limited to: Photographs/facial images, fingerprint images, iris images, voice samples, and signatures); and
- Details about images (i.e., capture date, reason fingerprinted, and location).

Encounter information may include:

- Scan of marked travel document page;
- Foreign partner point of contact information;
- Watchlist indicator, indicator of derogatory information, or reason for alert;
- Arrival, Departure, and/or Removal information (date and location);
- Transaction Control Numbers Associated with FBI fingerprint checks;
- Date/time of submission;
- Type of immigration form or non-biometric encounter;
- Date of immigration form or non-biometric encounter;

- Query results (match or no match);
- Error code; and
- Transaction Identifier Data (i.e., sending organization; timestamp; date; transaction type; case type; priority level; message origin; message destination; reference numbers (requesting participants subject specific reference number; or requesting participants event specific reference number); workstation; reason fingerprinted, such as entry, visa application, credentialing application, or apprehension; and any available encounter information, including an IDENT-generated encounter identification number (EID)).

BACKGROUND CHECK INFORMATION MAY INCLUDE:

- Results of criminal and national security background checks (i.e., positive or negative response; and positive responses are generally accompanied with the individual's criminal history and additional information explaining the results of the response); Unique Biometric Identifier (i.e., Fingerprint Identification Number (FIN) and Universal Control Number (formerly known as FBI Number)); and
- Logs associated with the requests of background checks, which may include requesting location and requesting person.

Document Production information may include:

- Identifying Transactional Information (i.e., transaction control number, book number);
- Biographical Information used for Document Production;
- Document Production Status;
- Benefit Card/Document Type;
- Class of Admission;
- Document Serial Number;
- Radio Frequency Identification (RFID) with USCIS Issued Document;
- Machine-readable Barcode;
- Production Site;
- Production Status; and
- Document Issuance Time/Date and Expiration Date.

RECORD SOURCE CATEGORIES:

Records are obtained from the categories of individuals included in this SORN. Information contained in this system may also be supplied by DHS, other U.S. Federal, state, tribal, or local government agencies, foreign government agencies, and international organizations. USCIS personnel may input information as they process a case, including information from internal and external sources, and to verify whether a benefit requestor or family is eligible for the benefit requested. Records covered by other

systems of records (or their successor systems) that are ingested and covered by this SORN include the following:

1. DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (Sept. 18, 2017);
2. DHS/USCIS-005 Intercountry Adoptions Security, 81 FR 78614 (Nov. 8, 2016);
3. DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), 77 FR 47411 (Aug. 8, 2012);
4. DHS/USCIS-007 Benefit Information System, 81 FR 72069 (Oct. 19, 2016);
5. DHS/USCIS-010 Asylum Information and Pre-Screening, 80 FR 74781 (Nov. 30, 2015);
6. DHS/USCIS-017 Refugee Case Processing and Security Screening Information, 81 FR 72075 (Oct. 19, 2016);
7. DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (Dec. 19, 2008);
8. DHS/ICE-011-Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, 81 FR 72080 (Oct. 19, 2016);
9. DHS/US-VISIT-001 DHS Automated Biometric Identification System (IDENT), 72 FR 31080 (June 5, 2007);
10. DHS/ALL-041 External Biometric Records (EBR) System of Records, 83 FR 17829 (April 24, 2018);
11. JUSTICE/FBI-002 The FBI Central Records System, 82 FR 24147 (May 25, 2017), and prior history (<https://www.justice.gov/opcl/doj-systems-records>);
12. JUSTICE/FBI-009 The Next Generation Identification (NGI) System, 81 FR 27283 (May 5, 2016), and 82 FR 24151 (May 25, 2017);
13. STATE-05 Overseas Citizens Services Records and Other Overseas Records, 81 FR 62235 (Sept. 8, 2016);
14. STATE-26 Passport Records, 80 FR 15653 (March 24, 2015);
15. STATE-39 Visa Records, 77 FR 65245 (Oct. 25, 2012);
16. STATE-59 Refugee Case Records, 77 FR 5865 (Feb. 6, 2012);
17. ODNI/NCTC-008 National Counterterrorism Center Terrorism Analysis Records, 72 FR 73895 (Dec. 28, 2007);
18. DoD/A0025-2 Defense Biometric Services, 74 FR 48237 (Sept. 22, 2009);
19. DoD/A0025-2 PMG (DFBA) Defense Biometric Identification Records System, 80 FR 8292 (Feb. 17, 2015); and
20. DoD/A0025-2a Defense Biometric Identification Records System, 74 FR 17840 (April 17, 2009).

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

Information in this system of records contains information relating to certain persons who have pending or approved benefit requests for special protected class status and should not be disclosed pursuant to a routine use unless disclosure is otherwise permissible under the confidentiality statutes, regulations, or policies applicable to that information. For example, information relating to persons who have applied for asylum or refugee status, have pending or approved benefit requests for protection under the Violence Against Women Act, Seasonal Agricultural Worker or Legalization claims, the Temporary Protected Status of an individual, and information relating to certain nonimmigrant visas. These confidentiality provisions do not prevent DHS from disclosing information to the Department of Justice (DOJ) and Offices of the United States Attorneys as part of an ongoing criminal or civil investigation.

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the DOJ, including Offices of the U.S. Attorneys, or other federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;
2. Any employee or former employee of DHS in his/her official capacity;
3. Any employee or former employee of DHS in his/her individual capacity when DOJ or DHS has agreed to represent the employee; or
4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is

necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when (1) DHS suspects or has confirmed that there has been a breach of the system of records; (2) DHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DHS (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

F. To another Federal agency or Federal entity, when DHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

G. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

H. To an appropriate Federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

I. To appropriate Federal, state, local, tribal, territorial, or foreign governments, as well as to other individuals and organizations during the course of an investigation by DHS or the processing of a matter under DHS's jurisdiction, or during a proceeding within the purview of the immigration and nationality laws, when DHS deems

that such disclosure is necessary to carry out its functions and statutory mandates.

J. To a former employee of DHS, in accordance with applicable regulations, for purposes of: Responding to an official inquiry by a Federal, state, or local government entity or professional licensing authority; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes when DHS requires information or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

K. To a coroner, in accordance with applicable law and regulations, for purposes of affirmatively identifying a deceased individual (whether or not such individual is deceased as a result of a crime).

L. To a Federal, state, or local government agency seeking to verify or ascertain the citizenship or immigration status of any individual within the jurisdiction of the agency for any purpose authorized by law.

M. To an appropriate domestic government agency or other appropriate authority for the purpose of providing information about an individual who has been or is about to be released from DHS custody who, due to a condition such as mental illness, may pose a health or safety risk to himself/herself or to the community. DHS will only disclose information about the individual that is relevant to the health or safety risk they may pose and/or the means to mitigate that risk (e.g., the individuals need to remain on certain medication for a serious mental health condition).

N. To foreign governments for the purpose of coordinating and conducting the removal of individuals to other nations under the INA; and to international, foreign, and intergovernmental agencies, authorities, and organizations in accordance with law and formal or informal international arrangements.

O. To DOJ FBI for the purpose of conducting name and fingerprint background checks in order to verify the identity of an individual and generate information used to grant or deny an immigration benefit request or other request.

P. To U.S. Department of State for the purpose of conducting biographic and biometric based searches for identity verification in order to process requests for benefits under the INA, and all other immigration and nationality laws including treaties and reciprocal agreements; or when DOS requires

information to consider and/or provide an informed response to a request for information from a foreign, international, or intergovernmental agency, authority, or organization about an alien or an enforcement operation with transnational implications.

Q. To U.S. Department of Defense for the purpose of biometric background checks to verify the identity of an individual and generate information used to grant or deny an immigration benefit request or other request.

R. To the Office of the Director of National Intelligence National Counterterrorism Center (ODNI/NCTC) and other Federal and foreign government intelligence or counterterrorism agencies when USCIS becomes aware of an indication of a threat or potential threat to national or international security, or when such use is to assist in anti-terrorism efforts and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

S. To an individual's prospective or current employer to the extent necessary to determine employment eligibility (for example, pursuant to the Form I-140, *Immigrant Petition for Alien Worker*).

T. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

DHS/USCIS stores records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be retrieved by any of the data elements listed above or a combination thereof. This may include, but is not limited to, name, date of birth, Alien Number, SSN, USCIS Online Account Number, and Receipt Number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

USCIS retains the records 100 years from the date of birth of the individual in accordance with NARA Disposition Authority Number DAA-0563-2013-0001-0005. USCIS collects and uses the information to verify the identity of the individual and support the background check process. The 100-year retention rate comes from the length of time USCIS may interact with a customer. Further, retaining the data for this period of time will enable USCIS to fight identity fraud and misappropriation of benefits.

USCIS generates secure identification documents to communicate adjudication decisions to the mailing address on file for the benefit requestor or his or her legal representative. USCIS systems that generate cards and documents retain data 10 years from the date of record creation in accordance with NARA Disposition Authority Number DAA-0566-2016-0014. Proof of benefits sent to the benefit requestor and returned to USCIS are retained by USCIS for up to one year in accordance with NARA Disposition Authority Number DAA-0566-2014-0005.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

DHS/USCIS safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. USCIS has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RECORD ACCESS PROCEDURES:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act, and consequently the JRA if applicable, because it may interfere with ongoing investigations and law enforcement activities. However, DHS will consider individual requests to determine whether or not information may be released. Thus, individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and Headquarters or component's FOIA Officer, whose contact information can be found at <http://www.dhs.gov/foia> under

“Contacts Information.” If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief FOIA Officer, Department of Homeland Security, Washington, DC 20528-0655. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about the individual may be available under the Freedom of Information Act.

When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the individual’s request must conform with the Privacy Act regulations set forth in 6 CFR part 5. The individual must first verify his or her identity, meaning that the individual must provide his or her full name, current address, and date and place of birth. The individual must sign the request, and the individual’s signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, an individual may obtain forms for this purpose from the Chief Privacy Officer and Chief FOIA Officer, <http://www.dhs.gov/foia> or 1-866-431-0486. In addition, the individual should:

- Explain why the individual believes the Department would have information on him or her;
- Identify which component(s) of the Department the individual believes may have the information about him or her;
- Specify when the individual believes the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records;

If an individual’s request is seeking records pertaining to another living individual, the first individual must include a statement from that individual certifying his/her agreement for the first individual to access his/her records.

Without the above information, the component(s) may not be able to conduct an effective search, and the individual’s request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES:

For records covered by the Privacy Act or covered JRA records, see “Records Access Procedures” above. Any individual, regardless of immigration status, may file a request to access his or her information under the

FOIA. Throughout the benefit determination process, and prior to USCIS making a determination to deny a benefit request, USCIS provides individuals with the opportunity to address and correct the information.

NOTIFICATION PROCEDURES:

See “Record Access Procedures.”

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

The Secretary of Homeland Security, pursuant to Secretary’s delegation number 15002 to the Director of USCIS to conduct certain law enforcement activities, when necessary to protect the national security and public safety, pursuant to 5 U.S.C. 552a(j)(2), is proposing to exempt this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); (f); and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f). When a record received from another system has been exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here.

HISTORY:

DHS/USCIS-002 Background Check Service, 72 FR 31082 (June 5, 2007); DHS/USCIS-003 Biometric Storage System, 72 FR 17172 (April 6, 2007).

Philip S. Kaplan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2018-16138 Filed 7-30-18; 8:45 am]

BILLING CODE 9111-97-P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

[Docket No. FR-6083-N-02]

Notice of a Federal Advisory Committee Meeting: Manufactured Housing Consensus Committee

AGENCY: Office of the Assistant Secretary for Housing—Federal Housing Commissioner, Department of Housing and Urban Development (HUD).

ACTION: Notice of a Federal Advisory Committee Meeting: Manufactured Housing Consensus Committee (MHCC).

SUMMARY: This notice sets forth the schedule and proposed agenda for a

meeting of the MHCC. The meeting is open to the public and the site is accessible to individuals with disabilities. The agenda provides an opportunity for citizens to comment on the business before the MHCC.

DATES: The meeting will be held on September 11 through September 13, 2018, 9:00 a.m. to 5:00 p.m. Eastern Standard Time (EST) daily.

ADDRESSES: The meeting will be held at the Holiday Inn Washington—Capitol, 550 C Street SW, Washington, DC 20024.

FOR FURTHER INFORMATION CONTACT:

Teresa B. Payne, Acting Administrator, Office of Manufactured Housing Programs, Department of Housing and Urban Development, 451 7th Street SW, Room 9166, Washington, DC 20410, telephone (202) 708-6423 (this is not a toll-free number). Persons who have difficulty hearing or speaking may access this number via TTY by calling the toll-free Federal Information Relay Service at 800-877-8339.

SUPPLEMENTARY INFORMATION:

Background

Notice of this meeting is provided in accordance with the Federal Advisory Committee Act, 5 U.S.C. App. 10(a)(2) through implementing regulations at 41 CFR 102-3.150. The MHCC was established by the National Manufactured Housing Construction and Safety Standards Act of 1974, 42 U.S.C. 5403(a)(3), as amended by the Manufactured Housing Improvement Act of 2000, (Pub. L. 106-569). According to 42 U.S.C. 5403, as amended, the purposes of the MHCC are to:

- Provide periodic recommendations to the Secretary to adopt, revise, and interpret the Federal manufactured housing construction and safety standards in accordance with this subsection;
- Provide periodic recommendations to the Secretary to adopt, revise, and interpret the procedural and enforcement regulations, including regulations specifying the permissible scope and conduct of monitoring in accordance with subsection (b);
- Be organized and carry out its business in a manner that guarantees a fair opportunity for the expression and consideration of various positions and for public participation.

The MHCC is deemed an advisory committee not composed of Federal employees.

Public Comment

Citizens wishing to make comments on the business of the MHCC are

required to be closed pursuant to 5 U.S.C. 552b(c)(1)(A) & (B). The second agenda item, a discussion of potential NSTAC study topics, will address areas of critical cybersecurity vulnerabilities and priorities for Government.

Government officials will share data with NSTAC members on initiatives, assessments, and future security requirements across public and private sector networks. The information will include specific vulnerabilities within cyberspace that affect the United States' information and communication technology infrastructures and proposed mitigation strategies. Disclosure of this information to the public would provide criminals with an incentive to focus on these vulnerabilities to increase attacks on the Nation's critical infrastructure and communications networks. As disclosure of this portion of the meeting is likely to significantly frustrate implementation of proposed DHS actions, it is required to be closed pursuant to 5 U.S.C. 552b(c)(9)(B).

Helen Jackson,
Designated Federal Officer for the NSTAC.
[FR Doc. 2017-19793 Filed 9-15-17; 8:45 am]
BILLING CODE 9110-9P-P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

Notice of Availability for Memorandum on Rescission of Deferred Action for Childhood Arrivals

AGENCY: Office of the Secretary, Department of Homeland Security.
ACTION: Notice of availability.

SUMMARY: In a memorandum dated September 5, 2017, the Acting Secretary of the Department of Homeland Security (DHS) rescinded the June 15, 2012 DHS memorandum entitled "Exercising Prosecutorial Discretion with Respect to Individuals Who Came to the United States as Children." The September 5, 2017 memorandum is available on the DHS Web site at the following location: <https://www.dhs.gov/news/2017/09/05/memorandum-rescission-daca>.

SUPPLEMENTARY INFORMATION: On June 15, 2012, then Secretary of Homeland Security Janet Napolitano issued a memorandum entitled "Exercising Prosecutorial Discretion with Respect to Individuals Who Came to the United States as Children." The 2012 memorandum established the policy known as Deferred Action for Childhood Arrivals (DACA).

On September 5, 2017, Acting Secretary of Homeland Security Elaine

Duke issued a memorandum entitled "Rescission of the June 15, 2012 Memorandum Entitled 'Exercising Prosecutorial Discretion with Respect to Individuals Who Came to the United States as Children.'" The September 5, 2017 memorandum rescinded the June 15, 2012 memorandum and directed DHS personnel to take all appropriate actions to execute a wind-down of the DACA program consistent with the parameters established in the memorandum. The September 5, 2017 memorandum is available on the DHS Web site at the following location: <https://www.dhs.gov/news/2017/09/05/memorandum-rescission-daca>.

Dated: September 11, 2017.

Elaine C. Duke,
Acting Secretary of Homeland Security.
[FR Doc. 2017-19794 Filed 9-15-17; 8:45 am]
BILLING CODE 9111-97-P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2017-0038]

Privacy Act of 1974; System of Records

AGENCY: Department of Homeland Security, Privacy Office.

ACTION: Notice of Modified Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to modify a current DHS system of records titled, "Department of Homeland Security/U.S. Citizenship and Immigration Services, U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection—001 Alien File, Index, and National File Tracking System of Records." This system of records contains information regarding transactions involving an individual as he or she passes through the U.S. immigration process, some of which may also be covered by separate Systems of Records Notices. DHS primarily maintains information relating to the adjudication of benefits, investigation of immigration violations, and enforcement actions in Alien Files (A-Files). Alien Files became the official file for all immigration records created or consolidated since April 1, 1944. Before A-Files, many individuals had more than one file with the agency. To streamline immigration recordkeeping, legacy Immigration and Naturalization Service issued each individual an Alien Number, allowing the agency to create a single file for each individual containing that individual's official

immigration record. DHS also uses other immigration files to support administrative, fiscal, and legal needs.

DATES: Submit comments on or before October 18, 2017. This modified system will be effective upon publication. New or modified routine uses will become effective October 18, 2017.

ADDRESSES: You may submit comments, identified by docket number DHS-2017-0038 by one of the following methods:

- **Federal e-Rulemaking Portal:** <http://www.regulations.gov>. Follow the instructions for submitting comments.
- **Fax:** 202-343-4010.
- **Mail:** Jonathan R. Cantor, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528-0655.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Donald K. Hawkins, (202) 272-8000, Privacy Officer, U.S. Citizenship and Immigration Services, 20 Massachusetts Avenue NW., Washington, DC 20529. For privacy questions, please contact: Jonathan R. Cantor, (202) 343-1717, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528-0655.

SUPPLEMENTARY INFORMATION: As DHS moves to conducting more immigration actions in an electronic environment and U.S. Citizenship and Immigration Services (USCIS) adjudicates more immigration benefits and requests for action in its USCIS Electronic Immigration System, DHS no longer considers the paper A-File as the sole repository and official record of information related to an individual's official immigration record. An individual's immigration history may be in the following materials and formats: (1) A paper A-File; (2) an electronic record in the Enterprise Document Management System or USCIS Electronic Immigration System; or (3) a combination of paper and electronic records and supporting documentation.

The Department of Homeland Security, therefore, is updating the "Department of Homeland Security/U.S. Citizenship and Immigration Services, U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection—001 Alien File, Index, and National File Tracking System of Records" notice to: (1) Redefine which records constitute the official record of an individual's immigration history to include the following materials and formats: (a) The paper A-File, (b) an electronic record in the Enterprise Document Management System or U.S. Citizenship and Immigration Services Electronic Immigration System, or (c) a

combination of paper and electronic records and supporting documentation; (2) clarify that data originating from this system of records may be stored in a classified paper A-File or classified electronic network; (3) provide updated system locations; (4) update category of individuals covered by this System of Records Notice, to include individuals acting as legal guardians or designated representatives in immigration proceedings involving an individual who is physically or developmentally disabled or severely mentally impaired (when authorized); Civil Surgeons who conduct and certify medical examinations for immigration benefits; law enforcement officers who certify a benefit requestors cooperation in the investigation or prosecution of a criminal activity; and interpreters; (5) expand the categories of records to include the following: country of nationality; country of residence; the USCIS Online Account Number; social media handles, aliases, associated identifiable information, and search results; and the Department of Justice (DOJ), Executive Office for Immigration Review and Board of Immigration Appeals proceedings information; (6) add and describe the purpose for the USCIS Electronic Immigration System, Electronic Document Management System, and Microfilm Digitization Application System; (7) expand the data elements used to retrieve records; (8) update the parameters for retention and disposal of A-Files; (9) add the Microfilm Digitization Application System retention schedule; (10) update system manager to Associate Director, Immigration Records and Identity Services; (11) update record source categories to include publicly available information obtained from the internet, public records, public institutions, interviewees, commercial data providers, and information obtained and disclosed pursuant to information sharing agreements; and (12) update routine use E to comply with new policy contained in Office of Management and Budget Circular A-108. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice. The exemptions for the existing system of records notice will continue to be applicable for this updated system of records notice. This modified system of records notice will be included in the DHS's inventory of record systems.

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the DHS U.S. Citizenship and Immigration Services

(USCIS), U.S. Immigration and Customs Enforcement (ICE), U.S. Customs and Border Protection (CBP) proposes to update and reissue a current DHS system of records titled, "DHS/USCIS-ICE-CBP-001 Alien File, Index, and National File Tracking System of Records."

DHS implements U.S. immigration law and policy through USCIS' processing and adjudication of applications and petitions submitted for citizenship, asylum, and other immigration benefits. USCIS also supports national security by preventing individuals from fraudulently obtaining immigration benefits and by denying applications from individuals who pose national security or public safety threats. DHS implements U.S. immigration policy and law through ICE's law enforcement activities and CBP's inspection and border security processes.

Legacy immigration and naturalization agencies previously collected and maintained information concerning all immigration and inspection interactions. Before Alien Files (A-Files), many individuals had more than one file with the agency requiring legacy personnel to search multiple records systems and indexes for all records pertaining to one individual. The former Immigration and Naturalization Services (INS) introduced A-Files and issued each individual an Alien Number (A-Number) allowing INS to create one file for each individual containing the entire agency's records for the subject. Legacy immigration case file records that were not consolidated into the A-File are still maintained since these records hold historical value and are shared with government agencies and members of the public who request this information for mission-related and genealogy purposes.

The Alien File, Index, and National File Tracking System of Records is the official record system that contains information regarding the transactions of an individual as he or she passes through the U.S. immigration process. Currently, A-Files may be maintained in two formats: Paper A-Files or electronic A-Files within the Enterprise Document Management System (EDMS). The official record will now take three possible forms: (1) Records contained within the paper A-File; (2) records contained within the electronic record from EDMS or USCIS Electronic Immigration System (USCIS ELIS); or (3) a combination of paper and electronic records and supporting documentation. The A-File serves as the official record of an individual's immigration history.

It is used in immigration proceedings before U.S. Department of Justice (DOJ) immigration judges and the Board of Immigration Appeals (BIA), and is the official record used in Federal court litigation and other official agency business transactions. USCIS is the custodian of the A-File and the documents contained within it that are derived from various systems belonging to USCIS, ICE, and CBP. All three components create, contribute information to, and use A-Files, hence this joint System of Records Notice (SORN).

A notice detailing this system of records was last published in the **Federal Register** on November 21, 2013, as the DHS/USCIS/ICE/CBP001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864. DHS is updating the DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records to include the following substantive changes: (1) Redefine which records constitute the official record of an individual's immigration history to include the following materials and formats: (a) The paper A-File, (b) the electronic A-File, or (c) a combination of paper and electronic records and supporting documentation; (2) clarify that data originating from this system of records may be stored in a classified paper A-File or classified electronic network; (3) provide updated system locations; (4) update category of individuals covered by this SORN to include individual acting as legal guardians or designated representatives in immigration proceedings involving individuals who are physically or developmentally disabled or severely mentally impaired (when authorized); Civil Surgeons who conduct and certify medical examinations for immigration benefits; and law enforcement officers who certify a benefit requestors cooperation in the investigation or prosecution of a criminal activity; and interpreters; (5) expand the categories of records to include country of nationality; country of residence; the USCIS Online Account Number; social media handles, aliases, associated identifiable information, and search results; and information regarding the DOJ Executive Office for Immigration Review (EOIR) and BIA proceedings; (6) add and describe the purpose of the USCIS ELIS, EDMS, and Microfilm Digitization Application System (MiDAS); (7) expand data elements used to retrieve records; (8) update the parameters for retention and disposal of paper A-Files and electronic A-Files; (9) include the MiDAS retention schedule; (10) change system

manager to Associate Director, Immigration Records and Identity Services (IRIS); (11) update record source categories to include publicly available information obtained from the internet, public records, public institutions, interviews, commercial data providers, and information shared obtained through information sharing agreements; and (12) update routine use E to comply with Office of Management and Budget Circular A-108.

Consistent with DHS's information sharing mission, information stored in the DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records may be shared with other DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, information contained within the DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records may be shared with appropriate Federal, State, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice. The exemptions for the existing system of records notice will continue to be applicable for this system of records notice. Additionally, this modified system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, and similarly, the Judicial Redress Act (JRA) provides a statutory right to covered persons to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records. In accordance with 5 U.S.C.

552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

SYSTEM NAME AND NUMBER:

Department of Homeland Security (DHS) U.S. Citizenship and Immigration Services (USCIS), U.S. Immigration and Customs Enforcement (ICE), U.S. Customs and Border Protection (CBP)—001 Alien File, Index, and National File Tracking System of Records.

SECURITY CLASSIFICATION:

Unclassified, sensitive, for official use only, and classified. The data may be retained in classified paper A-File or on classified networks. The nature and character of the underlying classification of these records will not change unless it is combined with classified information.

SYSTEM LOCATION:

Records are maintained in (1) paper A-Files; (2) electronic A-Files in EDMS and USCIS ELIS; (3) Central Index System (CIS); (4) MiDAS; and (5) National File Tracking System (NFTS). Other applications, as Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR) and the Person Centric Query Service (PCQS), may retrieve information from the aforementioned applications.

Paper A-Files: Paper A-Files are primarily located at the National Records Center in Lee's Summit, Missouri and component field offices. Paper A-Files may also be located at Headquarters, Regional, District, and other USCIS File Control Offices (FCO) throughout the United States and foreign countries as detailed on the agency's Web site, <http://www.uscis.gov>. A-Files may also be located at ICE and CBP offices and facilities.

EDMS: EDMS contains electronic A-Files.

USCIS ELIS: USCIS ELIS contains electronic A-Files. USCIS ELIS is an online, electronic account and case management system that stores information submitted or integrated into the system for the processing of specific applications, petitions, or requests. Submissions may originate in an electronic format or be converted to an electronic format from paper and include forms, supporting documentation associated with each submission notices of agency action (e.g., appointment notices, requests for evidence or originals, notices of intent to deny, or withdrawal notice and other final agency decisions) on a specific application, petition, or request,

whether filed directly online or received by USCIS in a paper format and subsequently scanned for integration into the USCIS ELIS. USCIS ELIS also stores the USCIS Online Account Number and biographic information about the individual filing a request for an immigration decision or agency action that can be used to retrieve information about other immigration requests that may have been filed by the individual.

CIS: CIS serves as a DHS-wide index of key information for A-Files (whether paper or electronic). CIS contains information on individuals who interact with DHS. The system contains biographic information on those individuals which can be used to retrieve additional information from other systems. However, A-Files are not contained in CIS.

MiDAS: MiDAS contains digitized copies of immigration-related records that were created between 1893 and 1975.

NFTS: NFTS has the location information for all A-File records (whether paper or electronic). NFTS allows DHS to track and log the movement of paper A-Files in a centralized database, and provide timely and accurate access to the immigration case file location. This system facilitates USCIS' ability to efficiently manage and streamline access to immigration files under its control.

The databases maintaining the above information are located within the DHS data center in the Washington, DC metropolitan area as well as throughout the country. Access to these electronic systems is possible at USCIS sites at Headquarters and in the field offices throughout the United States, at appropriate facilities under the jurisdiction of DHS, and other locations at which officers of DHS component agencies may be posted or operate to facilitate DHS's homeland security mission.

SYSTEM MANAGER(S):

Associate Director, Immigration Records and Identity Services, U.S. Citizenship and Immigration Services, Department of Homeland Security, 20 Massachusetts Avenue NW., Washington, DC 20529.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority for maintaining this system is in Sections 103 and 290 of the Immigration and Nationality Act (INA), as amended (8 U.S.C. 1103 and 1360), and the regulations issued pursuant thereto; and Section 451 of the Homeland Security Act of 2002 (Pub. L. 107-296), codified at 6 U.S.C. 271.

PURPOSE(S) OF THE SYSTEM:

The purpose of this system of records is to facilitate administration of benefits and enforcement of provisions under the INA and related immigration statutes. A-Files (whether paper or electronic), immigration case files, CIS, MiDAS, and NFTS are used primarily by DHS employees for immigration processing and adjudication, protection of national security, and administering and enforcing immigration and nationality laws and related regulations and policy. These records also assist DHS with detecting violations of immigration and nationality laws; supporting the referral of such violations for prosecution or other appropriate enforcement action; supporting law enforcement efforts and inspection processes at the U.S. borders; as well as to carry out DHS enforcement, immigration, intelligence, and or other homeland security functions.

The purpose of the A-File is to document and maintain the official record of an individual's immigration applications, petitions, and requests, as well as enforcement transactions as he or she passes through the U.S. immigration process. The official records in the A-Files consist of paper and electronic records of the individual's transactions through the immigration process including records of immigration benefit requests and requests for agency action filed with USCIS, but does not include all case processing and decisional data.

The purpose of the EDMS is to store the A-File electronically and to share the A-File more efficiently within DHS and with external agencies.

The purpose of USCIS ELIS is to maintain the A-File of certain paper- and electronically-filed benefit request forms with USCIS, in addition its electronic case processing, adjudication, and management functions. The associated information and data for cases maintained in USCIS ELIS for case processing, adjudication, and management functions are covered under other USCIS SORNs.

The purpose of CIS is to maintain a repository of electronic data that summarizes the history of an immigrant or non-immigrant in the adjudication process. In addition, CIS maintains information about individuals of interest to the U.S. Government for investigative purposes. Information contained within CIS is used for immigration benefit determination and for immigration law enforcement operations by USCIS, ICE, and CBP.

The purpose of MiDAS is to maintain a repository of historical immigration case files for use by government

agencies for mission-related purposes such as assisting in the determination to grant or deny a government benefit or to conduct law enforcement or other investigations. Furthermore, USCIS makes records of deceased subjects available to members of the public who request them for genealogy and other historical research purposes.

The purpose of NFTS is to account for the specific location of immigration files, and to track the request and transfer of immigration files.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

- Lawful permanent residents;
- Naturalized U.S. citizens;
- Individuals when petitioning for benefits under the INA, as amended, on behalf of another individual;
- Individuals acting as legal guardians or designated representatives in immigration proceedings involving an individual who has a physical or developmental disability or mental impairment (as authorized under the INA);
- Individuals who receive benefits under the INA;

• Individuals who are subject to the enforcement provisions of the INA;

• Individuals who are subject to the INA and:

○ Are under investigation by DHS for possible national security threats or threats to the public safety;

○ were investigated by DHS in the past;

○ are suspected of violating immigration-related criminal or immigration-related civil provisions of treaties, statutes, regulations, Executive Orders, and Presidential Proclamations administered by DHS, or

○ are witnesses and informants having knowledge of such violations;

• Relatives and associates of any of the individuals listed above who are subject to the INA;

• Individuals who have renounced their U.S. citizenship;

• Civil Surgeons who are required to conduct and certify medical examinations for immigration benefits; and law enforcement officers who certify a benefit requestor's cooperation in the investigation or prosecution of a criminal activity;

• Preparers assisting an individual seeking an immigration benefit or agency action under the INA;

• Interpreters assisting an individual seeking an immigration benefit or agency action under the INA;

• Attorneys or representatives recognized by USCIS or accredited by the BIA; or

• Law enforcement officers who certify a benefit requestor's cooperation

in the investigation or prosecution of a criminal activity.

Note: Individuals may fall within one or more of these categories.

CATEGORIES OF RECORDS IN THE SYSTEM:

A. A-Files contain official record material about each individual for whom DHS has created a record under the INA such as: Naturalization certificates; various documents and attachments (e.g., birth and marriage certificates); applications, petitions, and requests for immigration determinations or agency action under the immigration and nationality laws; reports of arrests and investigations; statements; other reports; records of proceedings before or filings made with the U.S. immigration courts and any administrative or federal district court or court of appeal; correspondence; and memoranda. Specific data elements may include:

- A-Numbers;
- Receipt file number(s);
- Full name and any aliases used;
- Physical and mailing addresses (to include U.S. and foreign);
- Phone numbers and email addresses;
- Social Security number (SSN);
- Date of birth;
- Place of birth (city, state, and country);
- Country of citizenship;
- Country of nationality;
- Country of residence;
- Gender;
- Physical characteristics (height, weight, race, eye and hair color, photographs, fingerprints);
- Government-issued identification information (*i.e.*, passport, driver's license):
 - Document type;
 - Issuing organization;
 - Document number; and
 - Expiration date;
 - Military membership and/or status;
 - Arrival/Departure information (record number, expiration date, class of admission, etc.);
 - Federal Bureau of Investigation (FBI) Identification Number/Universal Control Number;
 - Fingerprint Identification Number;
 - Immigration enforcement history, including, but not limited to, arrests and charges, immigration proceedings and appeals, and dispositions including removals or voluntary departures;
 - Immigration status;
 - Family history;
 - Travel history;
 - Education history;
 - Employment history;
 - Criminal history;
 - Professional accreditation information;

- Medical information;
- Information regarding the status of Department of Justice (DOJ), Executive Office of Immigration Review (EOIR) and (BIA) proceedings, if applicable;
 - Specific benefit eligibility information as required by the benefit being sought;
 - Social media handles and aliases, associated identifiable information, and search results; and
 - Cassette/audio tapes, audio-visual/videotapes, CDs, DVDs, or transcripts of immigration interviews.
- B. CIS contains information on those individuals who during their interactions with DHS have been assigned an A-Number. The system contains biographic information on those individuals, allowing DHS employees to quickly review the individual's immigration status. The information in the system can then be used to retrieve additional information on the individual from other systems. The information in the system can be used to request the paper A-File from the USCIS FCO that has custody of the A-File. Specific data elements may include:
 - A-Number(s);
 - Full name and any aliases used;
 - SSN;
 - Date of birth;
 - Place of birth (city, state, and country);
 - Country of citizenship;
 - Country of nationality;
 - Gender;
 - Government issued identification information (i.e., passport, driver's license):
 - Document type;
 - Issuing organization;
 - Document number;
 - Expiration date;
 - Arrival/Departure information (record number, expiration date, class of admission, etc.);
 - Immigration status;
 - Father and Mother's first name;
 - FBI Identification/Identification Universal Control Number;
 - Fingerprint Identification Number;
 - Immigration enforcement history, including arrests and charges, immigration proceedings and appeals, and dispositions including removals or voluntary departures; and
 - NFTS file location and status information.
 - C. EDMS contains official record material about each individual for whom DHS has created a record pursuant to the INA and the same information as contained in the as a paper A-File except for material that cannot be scanned from the paper A-File (e.g., cassette/audio tapes, audio-visual/video tapes, CDs, or DVDs).

D. USCIS ELIS contains official record information and material used to determine an outcome on an immigration application, petition, or request or request agency action, such as supporting documentation, and notices of agency action on the specific immigration request. USCIS ELIS also stores the USCIS Online Account Number biographic information about the individual seeking an immigration benefit or requesting agency action that can be used to retrieve information about other requests filed by the individual, and the electronic copy of the naturalization or certificate of citizenship. Specific data elements may include, but are not limited to:

- Full Name;
- Aliases;
- Physical and mailing addresses;
- A-Number;
- USCIS Online Account Number;
- SSN;
- Date of birth and/or death;
- Country of citizenship;
- Country of nationality;
- Country of residence;
- Place of birth;
- Gender;
- Marital status;
- Military membership or status;
- Phone and fax numbers (including mobile phone numbers);
- Email address;
- Immigration status;
- Biometric information (e.g., fingerprints, photographs, signature) and other information used to conduct background and security checks;
- Physical description (e.g., height, weight, eye color, hair color, race, ethnicity, identifying marks like tattoos or birthmarks);
- Government issued identification information (i.e., passport, driver's license):
 - Document type;
 - Issuing organization;
 - Document number; and
 - Expiration date;
 - Immigration benefit type and/or agency action requested (e.g., deferred action);
 - Supporting documentation as necessary (e.g., birth, marriage, and divorce certificates; licenses; academic diplomas and transcripts; appeals, requests for rehearing, and motions to reopen or reconsideration; explanatory statements; and unsolicited information submitted voluntarily by the individual seeking an immigration benefit or requesting agency action or family members in support of the request);
 - Notices and communications, including:
 - Requests for evidence;
 - Notices of intent to deny, fine, or terminate; and

- Proofs of benefit (e.g., Employment Authorization Card, Permanent Resident Card);
- Signature;
- Fee payment information (e.g., credit card number, *Pay.gov* Payment Tracking Number);
- Audio-visual recordings, including interviews and naturalization ceremonies;
- Travel history;
- Education history;
- Work history;
- Records regarding organization membership or affiliation;
- Family relationships (e.g., parent, spouse, sibling, child, other dependents);
- Information regarding the status of DOJ, EOIR and BIA proceedings, if applicable;
- Case processing information such as the date an immigration request was filed or received by USCIS; status of such a request; location of record; other control number when applicable; and fee receipt data;
- Representative information, including:
 - Name;
 - Law Firm/recognized organization;
 - Physical and mailing addresses;
 - Phone and fax numbers;
 - Email address;
 - Attorney Bar Card Number or equivalent;
 - Bar membership;
 - BIA representative accreditation authorization and expiration dates;
 - Law practice restriction(s) explanation; and
 - Signature.
- Preparer and Interpreter information, including:
 - Full Name;
 - Business or Organization name;
 - Physical and mailing addresses;
 - Phone and fax numbers;
 - Email address; and
 - Signature.
- E. NFTS contains the location of the A-File whether paper or electronic. Specific data elements include:
 - A-Number;
 - Receipt File Number;
 - Primary immigration file tracking number (e.g., A-Number, Receipt File Number, Certificate Number (C-Number), and Temporary Number (T-Number));
 - Location of the paper A-File and Receipt File within the USCIS FCO, as well as the history of who has maintained the paper A-File, including the component, section, and employee; and
 - Name of the USCIS FCO that has jurisdiction over a case maintained in USCIS ELIS and any transfer of jurisdiction to another USCIS office.

F. MiDAS is an online interactive application system that provides an automated means for searching an index to legacy immigrant records opened or indexed prior to 1975. The MiDAS Search Engine includes the Flexoline Index, documenting the issuance of A-Numbers to individuals between August 1940 and 1948, as well as a card index to physical A-Files opened between April 1, 1944 and 1975. MiDAS index data may be used to create or update a CIS record of an A-Number issued or A-File opened prior to 1975. Specific A-File index data elements may include, but are not limited to:

- A-Number;
- C-Number;
- Full name;
- Date of birth; and
- Place of birth (city, state, and country).

RECORD SOURCE CATEGORIES:

Basic information contained in DHS records is supplied by individuals on Department of State (DOS) and DHS applications and forms. Other information comes from publicly available information obtained from the Internet, public records, public institutions, interviewees, commercial data aggregators, inquiries or complaints from members of the general public and members of Congress, referrals of inquiries or complaints directed to the President or Secretary of Homeland Security, information shared through information sharing agreements, reports of investigations, sworn statements, correspondence, official reports, memoranda, and written referrals from other entities, including federal, state, and local governments, various courts and regulatory agencies, foreign government agencies, and international organizations.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

Information in this system of records contains information relating to persons who have pending or approved benefit requests for special protected classes and should not be disclosed pursuant to a routine use unless disclosure is otherwise permissible under the confidentiality statutes, regulations, or policies applicable to that information. For example, information relating to persons who have pending or approved benefit requests for protection under the Violence Against Women Act, Seasonal Agricultural Worker or Legalization claims, the Temporary Protected Status of an individual, and information relating to nonimmigrant visas protected under special confidentiality provisions

should not be disclosed pursuant to a routine use unless disclosure is otherwise permissible under the confidentiality statutes, regulations, or policies applicable to that information. These confidentiality provisions do not prevent DHS from disclosing information to the DOJ and Offices of the United States Attorney as part of an ongoing criminal or civil investigation.

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To DOJ, including Offices of the U.S. Attorneys, or other federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;
2. Any employee or former employee of DHS in his/her official capacity;
3. Any employee or former employee of DHS in his/her individual capacity when DOJ or DHS has agreed to represent the employee; or
4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS determines that information from this system of records is reasonably necessary and otherwise compatible with the purpose of collection to assist another federal recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach; or

2. DHS suspects or has confirmed that there has been a breach of this system of records; and (a) DHS has determined that as a result of the suspected or confirmed breach, there is a risk of harm to individuals, harm to DHS (including its information systems, programs, and operations), the Federal Government, or national security; and (b) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To appropriate Federal, State, tribal, local, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, when DHS believes the information would assist in enforcing applicable civil or criminal laws.

I. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation.

J. To an organization or person in either the public or private sector, either foreign or domestic, when there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, or when the information is relevant to the protection of life, property, or other vital interests of a person.

K. To clerks and judges of courts exercising naturalization jurisdiction for

the purpose of granting naturalization and administering naturalization oaths, and to enable such courts to determine eligibility for naturalization or grounds for revocation of naturalization.

L. To courts, magistrates, administrative tribunals, opposing counsel, parties, and witnesses, in the course of immigration, civil, or criminal proceedings before a court or adjudicative body when it is necessary or relevant to the litigation or proceeding and the following is a party to the proceeding or has an interest in the proceeding:

1. DHS or any component thereof; or
2. Any employee of DHS in his or her official capacity; or
3. Any employee of DHS in his or her individual capacity when the DOJ or DHS has agreed to represent the employee; or
4. The United States or any agency thereof.

M. To an attorney or representative (as defined in 8 CFR 1.2) who is acting on behalf of an individual covered by this system of records in connection with any proceeding before USCIS, ICE, or CBP or the DOJ EOIR, as required by law or as deemed necessary in the discretion of the Department.

N. To DOJ (including Offices of the United States Attorneys) or other federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when necessary to assist in the development of such agency's legal and/or policy position.

O. To DOS in the processing of petitions or applications for benefits under the INA, and all other immigration and nationality laws including treaties and reciprocal agreements; or when DOS requires information to consider and/or provide an informed response to a request for information from a foreign, international, or intergovernmental agency, authority, or organization about an alien or an enforcement operation with transnational implications.

P. To appropriate Federal, State, local, tribal, territorial, or foreign governments, as well as to other individuals and organizations during the course of an investigation by DHS or the processing of a matter under DHS's jurisdiction, or during a proceeding within the purview of the immigration and nationality laws, when DHS deems that such disclosure is necessary to carry out its functions and statutory mandates.

Q. To an appropriate Federal, State, local, tribal, territorial, or foreign government agency or organization, or international organization, lawfully

engaged in collecting law enforcement intelligence, whether civil or criminal, or charged with investigating, prosecuting, enforcing, or implementing civil or criminal laws, related rules, regulations, or orders, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence and the disclosure is appropriate to the proper performance of the official duties of the person receiving the information.

R. To an appropriate Federal, State, local, tribal, territorial, foreign, or international agency, if the information is relevant to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit.

S. To an appropriate Federal, State, local, tribal, territorial, foreign, or international agency, if DHS determines: (1) The information is relevant and necessary to that agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit; and (2) failure to disclose the information is likely to create a substantial risk to government facilities, equipment, or personnel; sensitive information; critical infrastructure; or public safety.

T. To appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to, or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk.

U. To an individual's current employer to the extent necessary to determine employment eligibility or to a prospective employer or government agency to verify whether an individual is eligible for a government-issued credential that is a condition of employment.

V. To a former employee of DHS, in accordance with applicable regulations, for purposes of: Responding to an official inquiry by a federal, state, or local government entity or professional licensing authority; or facilitating

communications with a former employee that may be necessary for personnel-related or other official purposes when DHS requires information or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

W. To the Office of Management and Budget (OMB) in connection with the review of private relief legislation as set forth in OMB Circular No. A-19 at any stage of the legislative coordination and clearance process as set forth in the Circular.

X. To the U.S. Senate Committee on the Judiciary or the U.S. House of Representatives Committee on the Judiciary when necessary to inform members of Congress about an alien who is being considered for private immigration relief.

Y. To a Federal, State, tribal, or local government agency and/or to domestic courts to assist such agencies in collecting the repayment of loans, or fraudulently or erroneously secured benefits, grants, or other debts owed to them or to the U.S. Government, or to obtain information that may assist DHS in collecting debts owed to the U.S. Government.

Z. To an individual or entity seeking to post or arrange, or who has already posted or arranged, an immigration bond for an alien, to aid the individual or entity in (1) identifying the location of the alien; (2) posting the bond; (3) obtaining payments related to the bond; or (4) conducting other administrative or financial management activities related to the bond.

AA. To a coroner for purposes of affirmatively identifying a deceased individual (whether or not such individual is deceased as a result of a crime).

BB. Consistent with the requirements of the INA, to the Department of Health and Human Services (HHS), the Centers for Disease Control and Prevention (CDC), or to any state or local health authorities, to:

1. Provide proper medical oversight of DHS-designated Civil Surgeons who perform medical examinations of both arriving aliens and of those requesting status as lawful permanent residents; and

2. Ensure that all health issues potentially affecting public health and safety in the United States are being or have been, adequately addressed.

CC. To a Federal, State, local, tribal, or territorial government agency seeking to verify or ascertain the citizenship or immigration status of any individual within the jurisdiction of the agency for any purpose authorized by law.

DD. To the Social Security Administration (SSA) for the purpose of issuing a SSN and card to an alien who has made a request for a SSN as part of the immigration process and in accordance with any related agreements in effect between the SSA, DHS, and DOS entered into pursuant to 20 CFR 422.103(b)(3), 422.103(c)(3), and 422.106(a), or other relevant laws and regulations.

EE. To Federal and foreign government intelligence or counterterrorism agencies or components when DHS becomes aware of an indication of a threat or potential threat to national or international security, or when such use is to conduct national intelligence and security investigations or assist in anti-terrorism efforts.

FF. To third parties to facilitate placement or release of an individual (e.g., at a group home, homeless shelter) who has been or is about to be released from DHS custody, but only such information that is relevant and necessary to arrange housing or continuing medical care for the individual.

GG. To an appropriate domestic government agency or other appropriate authority for the purpose of providing information about an individual who has been or is about to be released from DHS custody who, due to a condition such as mental illness, may pose a health or safety risk to himself/herself or to the community. DHS will only disclose information about the individual that is relevant to the health or safety risk they may pose and/or the means to mitigate that risk (e.g., the individual's need to remain on certain medication for a serious mental health condition).

HH. To foreign governments for the purpose of coordinating and conducting the removal of individuals to other nations under the INA; and to international, foreign, and intergovernmental agencies, authorities, and organizations in accordance with law and formal or informal international arrangements.

II. To a Federal, State, local, territorial, tribal, international, or foreign criminal, civil, or regulatory law enforcement authority when the information is necessary for collaboration, coordination, and de-confliction of investigative matters, prosecutions, and/or other law enforcement actions to avoid duplicative or disruptive efforts and to ensure the safety of law enforcement officers who may be working on related law enforcement matters.

JJ. To the DOJ Federal Bureau of Prisons and other Federal, State, local, territorial, tribal, and foreign law enforcement or custodial agencies for the purpose of placing an immigration detainee on an individual in that agency's custody, or to facilitate the transfer of custody of an individual from DHS to the other agency. This will include the transfer of information about unaccompanied minor children to HHS to facilitate the custodial transfer of such children from DHS to HHS.

KK. To Federal, State, local, tribal, territorial, or foreign governmental or quasi-governmental agencies or courts to confirm the location, custodial status, removal, or voluntary departure of an alien from the United States, in order to facilitate the recipients' exercise of responsibilities pertaining to the custody, care, or legal rights (including issuance of a U.S. passport) of the removed individual's minor children, or the adjudication or collection of child support payments or other debts owed by the removed individual.

LL. To a Federal, State, tribal, territorial, local, international, or foreign government agency or multilateral governmental organization for the purpose of consulting with that agency or entity: (1) To assist in making a determination regarding redress for an individual in connection with the operations of a DHS component or program; (2) for the purpose of verifying the identity of an individual seeking redress in connection with the operations of a DHS component or program; or (3) for the purpose of verifying the accuracy of information submitted by an individual who has requested such redress on behalf of another individual.

MM. To family members, guardians, committees, friends, or other agents identified by law or regulation to receive notification, decisions, and other papers as provided in 8 CFR 103.8 from DHS or EOIR following verification of a familial or agency relationship with an alien when DHS is aware of indicia of incompetency or when an immigration judge determines an alien is mentally incompetent.

NN. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific

information in the context of a particular case would constitute a clearly unwarranted invasion of personal privacy.

OO. To domestic governmental agencies seeking to determine the immigration status of persons who have applied to purchase/obtain a firearm in the United States, pursuant to checks conducted on such persons under the Brady Handgun Violence Prevention Act or other applicable laws.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

DHS/USCIS retrieves records by searching in CIS using the following data alone or in any combination:

- A-Number;
- Full name;
- Alias;
- Sounds-like name with or without date of birth;
- Certificate of Citizenship or Naturalization Certificate number;
- Driver's License number;
- FBI Identification/Universal Control Number;
- Fingerprint Identification Number;
- I-94 admission number;
- Passport number;
- SSN; or
- Travel Document number.

DHS/USCIS retrieves records by searching electronic A-Files in EDMS by any of the following fields alone or in any combination:

- A-Number;
- Last name;
- First name;
- Middle name;
- Aliases;
- Date of birth;
- Country of birth;
- Gender; and
- Through a full text-based search of records contained in the electronic A-File (based on optical character recognition of the scanned images).

DHS/USCIS retrieves records by searching in USCIS ELIS using the following data alone or in any combination:

- Full Name;
- Aliases;
- A-Number;
- USCIS Online Account Number;
- Date of birth;
- Immigration benefit type and/or agency action requested (e.g., deferred action);

- Fee receipt data;
- Date benefit request was filed;
- Date benefit request was received;
- Representative name;
- Preparer name; and
- Interpreter name.

DHS/USCIS retrieves the location of A-Files, whether paper or electronic, by searching in NFTS using the following data:

- A-Number;
- USCIS Online Account Number; or
- Receipt File Number.

DHS/USCIS retrieves genealogy records and requests in MiDAS by searching the following data alone or in any combination:

- Requestor's first name;
- Requestor's last name;
- Requestor's Case and/or Control Number;
- Record subject's A-Number or immigration case file number;
- Record subject's first name;
- Record subject's last name; and
- Record subject's alias.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

The official A-File record may take three possible forms: (1) Records contained within the paper A-File; (2) records contained within the electronic record from EDMS or USCIS ELIS; or (3) a combination of paper and electronic records and supporting documentation. A-File records are maintained in accordance with N1-566-08-11. DHS/USCIS transfers A-Files to the custody of NARA 100 years after the individual's date of birth.

CIS records are maintained in accordance with N1-566-10-01. CIS is an internal DHS-mission critical system that contains records that serve as a finding aid to agency case files. Records in CIS are permanently retained because they are the index of the A-File, summarize the history of an immigrant in the adjudication process, and identify the A-File location(s).

NFTS records are maintained in accordance with N1-566-06-01. NFTS records are temporary and deleted when they are no longer needed for agency business. NFTS records associated with an A-File will be retained on a permanent basis even after the A-File has been retired to NARA to retain accurate recordkeeping. Other immigration case files with a shorter retention period will have the associated NFTS record destroyed or deleted once the file has been destroyed.

MiDAS information (data and electronic images) pertaining to correspondence with the public and government requestor is retained and disposed every six years in accordance

with the NARA General Records Schedules 4.2 and 14. The immigration case files contained in MiDAS are retained permanently. Records are transferred to NARA after 100 years after the last completed action.

Records replicated on the unclassified and classified networks for analysis and vetting will follow the same retention schedule.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

DHS/USCIS safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. USCIS has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RECORD ACCESS PROCEDURES:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act, and those of the Judicial Redress Act (JRA) if applicable, because it is a law enforcement system. However, DHS/USCIS will consider individual requests to determine whether or not information may be released. Thus, individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and USCIS Freedom of Information Act (FOIA) Officer, whose contact information can be found at <http://www.dhs.gov/foia> under "Contacts Information." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, Washington, DC 20528-0655. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about you may be available under the FOIA.

When seeking records about yourself from this system of records or any other Departmental system of records, your request must conform with the Privacy Act regulations set forth in 6 CFR part 5. You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your

request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, <http://www.dhs.gov/foia> or 1-866-431-0486. In addition, you should:

- Explain why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records.

If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without the above information, the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES:

For records covered by the Privacy Act or covered JRA records, see "access procedures" above.

NOTIFICATION PROCEDURES:

See "Record Access procedure."

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2): 5 U.S.C. 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (e)(12), (f), (g)(1), and (h). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1) and (k)(2): 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f).

When this system receives a record from another system exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here.

HISTORY:

DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking

System of Records, 78 FR 69864 (Nov. 21, 2013); Alien File, Index, and National File Tracking SORN, 76 FR 34233 (Jun. 13, 2011); Alien File (A-File) and Central Index System (CIS) Systems of Records 78 FR 1755 (Jan. 16, 2007).

Jonathan R. Cantor,
Acting Chief Privacy Officer, Department of Homeland Security.
[FR Doc. 2017-19365 Filed 9-15-17; 8:45 am]
BILLING CODE 9111-97-P

DEPARTMENT OF HOMELAND SECURITY

U.S. Immigration and Customs Enforcement

[OMB Control Number 1653-0038]

Agency Information Collection Activities: Student and Exchange Visitor Information System (SEVIS); Extension, Without Change, of a Currently Approved Collection

AGENCY: U.S. Immigration and Customs Enforcement, Department of Homeland Security.

NOTICE: 60-day notice.

SUMMARY: The Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement (ICE) will be submitting the following information collection request to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995. The information collection is published in the **Federal Register** to

obtain comments from the public and affected agencies.

DATES: Comments are encouraged and will be accepted for sixty days until November 17, 2017.

ADDRESSES: Written comments and suggestions regarding items contained in this notice and especially with regard to the estimated public burden and associated response time should be directed the Department of Homeland Security (DHS), PRA Clearance Officer, U.S. Immigration and Customs Enforcement, 801 I Street NW., Mailstop 5800, Washington, DC 20536-5800.

SUPPLEMENTARY INFORMATION: Written comments and suggestions from the public and affected agencies concerning the proposed collection of information should address one or more of the following four points:

(1) Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

(2) Evaluate the accuracy of the agencies estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;

(3) Enhance the quality, utility, and clarity of the information to be collected; and

(4) Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology,

e.g., permitting electronic submission of responses.

Overview of This Information Collection

(1) *Type of Information Collection:* Extension, without change, of a currently approved information collection.

(2) *Title of the Form/Collection:* Student and Exchange Visitor Information System (SEVIS).

(3) *Agency form number, if any, and the applicable component of the Department of Homeland Security sponsoring the collection:* Forms I-17 and I-20; U.S. Immigration and Customs Enforcement.

(4) *Affected public who will be asked or required to respond, as well as a brief abstract:* Primary Non-profit institutions and individuals or households. SEVIS is an Internet-based data-entry, collection and reporting system. It collects information on SEVP-certified schools via the Form I-17, "Petition for Approval of School for Attendance by Nonimmigrant Student," and collects information on the F and M nonimmigrant students that the SEVP-certified schools admit into their programs of study via the Forms I-20s: "Certificate of Eligibility for Nonimmigrant (F-1) Student Status—For Academic and Language Students" and "Certificate of Eligibility for Nonimmigrant (M-1) Student Status—For Vocational Students".

(5) *An estimate of the total number of respondents and the amount of time estimated for an average respondent to respond:*

Number of respondents	Form name/Form No.	Average burden per response (in hours)
280,000	Certificate of Eligibility for Nonimmigrant (F-1) Student Status—For Academic and Language Students/ICE Form I-20 (Students).	0.5
90,000	Certificate of Eligibility for Nonimmigrant (M-1) Student Status—For Academic and Language Students/ICE Form I-20 (Spouse/Dependents).	0.5
280,000	Optional Practical Training 12 Month Request/No Form	0.083
12,000	Optional Practical Training 17 Month Extension Request/No Form	0.083
5,525	Maintenance of SEVP Certification/ICE Form I-17	4

(6) *An estimate of the total public burden (in hours) associated with the collection:* 1,027,884 annual burden hours.

Dated: September 12, 2017.

Scott Elmore,

PRA Clearance Officer, Office of the Chief Information Officer, U.S. Immigration and Customs Enforcement, Department of Homeland Security.

[FR Doc. 2017-19713 Filed 9-15-17; 8:45 am]

BILLING CODE 9111-28-P

NOTICE OF OFFICE OF MANAGEMENT AND BUDGET ACTION

Date 08/16/2024

Department of Homeland Security
 U.S. Citizenship and Immigration Services

FOR CERTIFYING OFFICIAL: Robert Dorr
 FOR CLEARANCE OFFICER: Tyrone Huff

In accordance with the Paperwork Reduction Act, OMB has taken action on your request received
08/15/2024

ACTION REQUESTED: New collection (Request for a new OMB Control Number)

TYPE OF REVIEW REQUESTED: Emergency

ICR REFERENCE NUMBER: 202407-1615-002

AGENCY ICR TRACKING NUMBER: I-131F

TITLE: I-131F, Application for Parole in Place for Certain Noncitizen Spouses and Stepchildren of U.S. Citizens

LIST OF INFORMATION COLLECTIONS: See next page

OMB ACTION: Approved with change

OMB CONTROL NUMBER: 1615-0161

The agency is required to display the OMB Control Number and inform respondents of its legal significance in accordance with 5 CFR 1320.5(b).

EXPIRATION DATE: 02/28/2025

DISCONTINUE DATE:

BURDEN:	RESPONSES	HOURS	COSTS
Previous	0	0	0
New	1,100,000	1,285,185	283,250,000
Difference			
Change due to New Statute	0	0	0
Change due to Agency Discretion	1,100,000	1,285,185	283,250,000
Change due to Agency Adjustment	0	0	0
Change due to PRA Violation	0	0	0

TERMS OF CLEARANCE: OIRA approves the emergency request for a period of six months, contingent on the following: USCIS will publish a 60-day Federal Register notice to begin normal processing under the PRA within 60 days of this approval; USIS will implement certain de minimis changes requested by EOP reviewers as soon as practically possible but prior to the expiration of the 6 month emergency period; and as part of the 3-year renewal PRA package, USCIS will incorporate certain agreed-upon substantive form changes flagged by EOP reviewers during OIRA review of the Form I-131F filing guide.

OMB Authorizing Official: Dominic J. Mancini
 Deputy Administrator,
 Office Of Information And Regulatory Affairs

List of ICs			
IC Title	Form No.	Form Name	CFR Citation
Form I-131F, Application for Parole in Place for Certain Noncitizen Spouses and Stepchildren of U.S. Citizens	I-131F (Online E-File)	Application for Parole in Place for Certain Noncitizen Spouses and Stepchildren of U.S. Citizens	8 CFR 274a.12(c)(11)
Biometrics			8 CFR 103